2006

Survivable design in WDM mesh networks

Wensheng He
Iowa State University

Survivable design in WDM mesh networks

by

Wensheng He

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Computer Engineering

Program of Study Committee:
Arun K. Somani, Major Professor
Manimaran Govindarasu
Ahmed E. Kamal
Doug Jacobson
Lu Ruan

Iowa State University

Ames, Iowa

2006

Graduate College
Iowa State University

This is to certify that the doctoral dissertation of

Wensheng He

has met the dissertation requirements of Iowa State University

Signature was redacted for privacy.

Major Professor

Signature was redacted for privacy.

For the Major Program

DEDICATION

To my parents and my wife for their support, encouragement, and love.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor, Prof. Arun K. Somani, for his guidance and encouragement throughout this work. Without his encouragement and support I would not have been able to complete this work.

I would like to thank my committee members, Prof. Ahmed E. Kamal, Prof. Manimaran Govindarasu, Prof. Doug Jacobson, and Prof. Lu Ruan, for their valuable suggestions and comments to improve the quality of this dissertation. Special thanks to Prof. Lu Ruan for reading my dissertation meticulously and offering insightful comments.

I would like to thank my fellow graduate students for their helps: Murari Sridharan, Srinivasan Ramasubramanian, Tao Wu, Jing Fang, Srivatsan Balasubramanian, Jinran Chen, Michael T Frederick, and David Lastine. Special thanks to Jing Fang and Srivatsan Balasubramanian for the opportunity of working together and valuable discussions I had with them. I would also like to thank my friend Jim Robbins for his support and friendship during the years of my stay in Ames.

Finally, I thank my parents and my wife Qun Xiang for their invaluable support and encouragement.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

This dissertation addresses several important survivable design issues in WDM mesh networks.

We first consider single link failure scenarios. To achieve both high efficiency in capacity utilization and fast restoration are primary goals of survivable design in optical networks. Shared backup path protection has been shown to be efficient in terms of capacity utilization, due to the sharing of backup capacity. However, sharing of backup capacity also complicates the restoration process, and leads to slow recovery. Ring-type protection in mesh topology, on the other hand, has the advantage of fast restoration. The p-cycle scheme is the most efficient ring-type protection method in terms of capacity utilization. Recently, the concept of pre-cross-connected protection was proposed to increase the recovery speed of shared path protection. We overview these protection methods and discuss their failure recovery processes. The recovery time of these schemes are compared analytically. We formulate integer programming optimization problems for three protection methods in static traffic scenario, considering wavelength continuity constraint. We investigate the effect of network connectivity on the performance of capacity utilization of the methods by experimenting on topologies with different average nodal degrees.

Dynamically provisioning connections, i.e. lightpaths are established on demand as connection requests arrive at the network and torn down when connections are terminated is becoming more important in backbone transport network. Survivable design for dynamic traffic using p-cycle technique has the potential to achieve both fast recovery and capacity efficiency. We develop a p-cycle based scheme to deal with dynamic traffic in WDM networks. We use a two-step approach. In first step, we find a set of p-cycles to cover the network and reserve

enough capacity in p-cycles. By doing this, we provision the network built-in resources to be two parts: protection resources and resources available for accommodating the working traffic. The design also ensures that the p-cycles are preconfigured. In second step, we route the requests as they randomly arrive one by one. We propose two routing algorithms. Compared to the shared path protection, in which a primary path and backup path is determined for each request as it arrives, the p-cycle based protection considers the protection in the network as a whole in one step. The p-cycle based design has the advantage of fast recovery, less control signaling, less dynamic state information to be maintained. To evaluate the blocking performance of proposed method, we compare it with shared backup path protection by extensive simulations.

Although the failure of single component such as a link or a node is the most common failure scenario, it is possible to have multiple links fail simultaneously. We consider double-link failure scenario in which two links can fail simultaneously. We propose a path-based protection method for two-link failures in mesh optical networks. We identify the scenarios where the backup paths can share their wavelengths without violating 100% restoration guarantee (backup multiplexing). We use integer linear programming to optimize the total capacity requirement for both dedicated- and shared-path protection schemes. Numerical results indicate that, backup multiplexing significantly improves the efficiency of total capacity utilization.

The recently proposed *light trail* architecture offers a promising candidate for carrying IP centric traffic over optical networks. The survivable design is a critical part of the integral process of network design and operation. We propose and compare two protection schemes, namely *connection based protection* and *link based protection*, that can achieve 100% protection against single link failure. The survivable light trail design problem using connection based protection model is solved using a two-step approach.

CHAPTER 1. Introduction

1.1 Optical Networks: A Brief History

With the rapid maturation and the integration of computer and communication technologies, telecommunication networks have change the world dramatically. The ever-increasing demand for bandwidth fueled by explosive growth of Internet and corporate intranet traffic has been the major driver for the technology innovation and evolution of telecommunication networks. Optical fiber medium has become the dominant transport medium in telecommunication systems, as it is capable of providing high-bandwidth service cost-effectively. New multiplexing techniques such as WDM (Wavelength Division Multiplexing) have been developed to utilize the fiber capacity more efficiently. WDM harnesses the vast transmission bandwidth of optical fiber into non-overlapping wavelength channels and enables data transmission over these channels simultaneously. Each of these channels operates at a transmission rate compatible with current peak electronic rates. The evolution of optical networks are often classified into two generations [1]:

First Generation Optical Networks: In first-generation optical networks, optical fiber was used merely as a replacement for copper as the transmission medium, in view of its huge bandwidth capability. SONET (Synchronous Optical Network) and SDH (Synchronous Digital Hierarchy) are a set of related standards for synchronous data transmission over fiber optic networks. SONET is the United States version of the standard published by the ANSI (American National Standards Institute). SDH is the international version of the standard published by the ITU (International Telecommunications Union).

The important feature of synchronous mode makes it easy to extract low speed streams from

a high speed stream in SONET/SDH networks. All the clocks in the network are synchronized to a single external clock. The bit rates defined in SONET/SDH are integral multiples of the basic rate. Another significant advantage of SONET/SDH is that they define standard optical interfaces that enables multi-vendor interoperability. SONET/SDH also have specific protection schemes to provide high-availability of services. In general, they can achieve restoration time after failure at the order of 50ms.

The major problem with first-generation optical networks is that the data sent over the network along multiple links undergoes optical-to-electronic conversion and vice verse at each intermediate node before reaching its destination. As a consequence, the network does not provide protocol transparency, that is, the capability of supporting multiple transmission rates and modulation formats. Data processing at each intermediate node also results in additional overhead. These are the key drivers for second-generation optical networks.

Second-Generation Optical Networks: With the advances in optical technologies, it was realized that optical networks are capable of providing more functions than just point-to-point transmission. In second-generation optical networks, some of the switching and routing functions that were performed by electronics are incorporated into optical domain. For example, the electronics at a node only need to handle the data intended for that node. The data that is being passed through that node on to other nodes in the network will be routed through in the optical domain. Therefore, data can sent from one node to another entirely in the optical domain, providing complete transparency.

Second-generation WDM optical networks that provide circuit-switched light path service have been deployed in the backbone networks. Optical-packet-switching is thought to still be premature in the current state.

1.2 Wavelength-Routed WDM networks

In wavelength-routed WDM networks, nodes are capable of routing different wavelengths at an input port to different output ports using *optical cross-connects*. The switching is done

in the optical domain. A *lightpath* is an optical communication path between two nodes, established by allocating a wavelength throughout the route of the transmitted data [2]. *Wavelength continuity constraint* is a property that requires that a lightpath has to use same wavelength on every link in its path, unless the wavelength conversion capability is provided within the network. *Wavelength conversion* is a mechanism by which an optical signal from one wavelength is converted to another. A device that performs such a conversion is referred to as *wavelength convertor*. An alternative for wavelength conversion is to use *multifiber networks*, which employs multiple fibers in a link.

1.2.1 Multi-Layered Architecture

In wavelength-routed WDM networks, a new network layer, called the optical layer or WDM layer, is introduced into the layered architecture shown in Figure 1.1 [1]. Different carriers can choose different layering strategies to realize their networks and optimize the performance. Incumbent carriers may use their large installed SONET/SDH gear, and the digital crossconnects. An IP (Internet Protocol) service provider may choose to use IP as the basic network transport layer without using SONET/SDH. Carriers that provide QoS (Quality of Services) may use ATM (Asynchronous Transfer Mode) as their transport technology. Underneath these layers is the optical layer, which provides lightpaths to the higher layers. Optical layer also provides protection mechanisms to recover from the failures. The advantages of optical layer protection will be discussed in the following section.

1.3 Survivability in Optical Networks

As wavelength routing paves the way for network throughputs of possibly hundreds of Tb/s, network survivability assumes critical importance. A short network outrage can lead to huge data loss. Survivability refers to the ability of the network to reconfigure and reestablish communication upon failures. According to [1], the overall availability requirements are of the order of 99.999% or higher.

The basic types of network failures generally considered are link and node failure. Cable

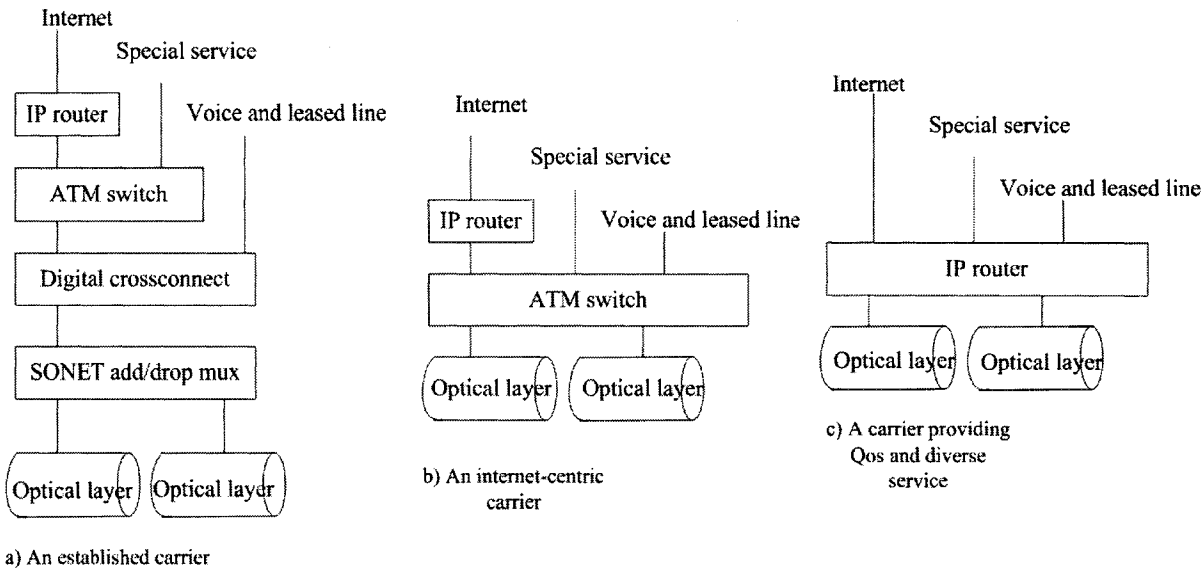

Figure 1.1 Different network layered architectures.

cuts that cause link failure are common in optical networks. Node failure usually is due to equipment failure at a node. Channel failure is another type of failure that is unique to WDM networks. A channel failure is usually caused by the failure of transmitting or receiving equipment operating on that channel.

1.3.1 Protection and Restoration

The survivability techniques that have been proposed and used in optical networks can be classified into two general categories: preplanned protection and dynamic restoration. Preplanned protection refers to the fact that recovery from network failure is based on preplanned schemes and resources. In preplanned protection, some resources are reserved for recovery from failures at either network design or connection setup time, and kept idle when there is no failure. Upon the failure occurs, reserved resources will be used to recover from the failure according to protection protocols. In contrast, in dynamic restoration, the resources used for recovery from failure are not reserved at the time of connection establishment, but are discov-

ered dynamically when a failure occurs. Dynamic restoration uses resources more efficiently than preplanned protection. On the other hand, the restoration time for dynamic restoration is usually longer, and 100% service recovery cannot be guaranteed because sufficient spare capacity may not be available at the time of failure.

Preplanned protection is the prefered approach. Most of the research focus on preplanned protection. Figure 1.2 shows a classification of survivable design techniques used in Non-WDM (SONET) optical networks as well as those for WDM networks [3, 4, 5].

1.3.2 Why Optical Layer Protection

Given the factor that the IP, ATM, and SONET layers shown in Figure 1.1 all incorporate protection and restoration mechanisms, a natural question is why the optical layer protection is needed. The following are the main reasons to provide protection in the new WDM layer [1].

- Layers operating above the optical layer may not be fully able to provide the protection functions as needed in the network. For example, fault tolerance in IP layer based on rerouting is cumbersome and not fast enough to provide QoS. If we adopt the layer architecture in which IP directly operates above WDM without using SONET, the optical layer protection is needed to provide fast restoration.

- Optical layer protection is more efficient in handling certain types of failures, such as fiber cuts. A single fiber cut leads to failure of multiple SONET streams. If each these streams are to be restored independently by the SONET layer, a large number of alarms will flood the network management system. This can be avoided if optical layer protection is used to recover the failure.

- Optical layer protection and restoration may be used to provide an additional resilience in the network. For example, optical layer can be used to provide resilience against multiple failures.

- Significant cost savings can be obtained by making use of optical layer protection and restoration.

It should be clear that optical layer protection cannot handle any faults in the higher layer of network. For example, it cannot handle the failure of a SONET ADM attached to the optical network. Because of the property of protocol transparency, the optical layer may be unaware of what exactly is carried on the lightpaths, and therefore, cannot monitor the traffic to sense the degradation.

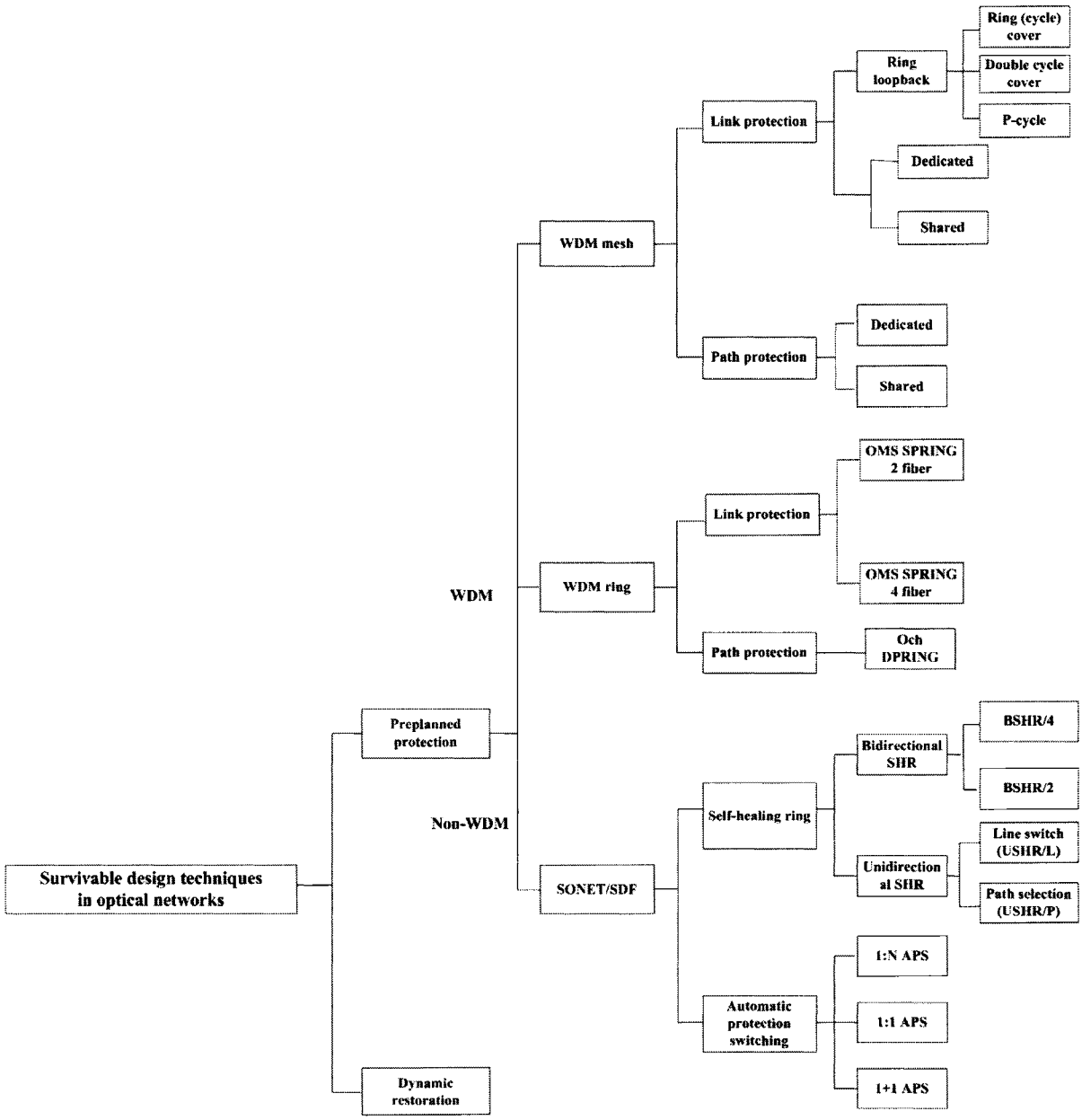

Figure 1.2 Survivable design techniques in optical networks.

1.3.3 Protection Schemes in Non-WDM networks

To trace the evolution of protection methods in optical networks, we first look at protection schemes in Non-WDM optical networks. APS (Automatic protection switching) and SHR (self-healing ring) are the most common preplanned protection schemes used in non-WDM optical networks [3].

APS is typically used to handle link failures. Based on the assignment of protection resources, there are three main architectures: 1+1, 1:1, and 1:N APS. In 1+1 APS, a protection link is provided for every working link. The source node transmits the data on both working and protection links. The receiver at the destination node compares the two signals and chooses the better one. In 1:1 APS, every working link has a protection link. But the protection link is either idle or used to carry low-priority traffic when the working link is not failed. The source and destination nodes switch to the protection link only when the working link is failed. In 1:N APS, N working links share a single protection link. When more than one link fail simultaneously, the traffic routed to the protection links can be decided according to preassigned priorities.

SHR can handle both link and node failures. Networks are designed to have ring architecture. There are two types of SHR in SONET system: USHR (Unidirectional SHR) and BSHR (Bidirectional SHR). In USHR, the normal traffic flow goes around the ring is in one direction, whereas in BSHR, working traffic flows in both directions.

USHR is either line protection switched (USHR/L) or path protection switched (USHR/P). In USHR/L, two nodes adjacent to a failure switch the affected traffic to the protection ring when there is a failure (link or node). This is also called *loopback*. In USHR/P, the signals for every connection are transmitted on both rings. When a failure occurs, the ADM at each node chooses the better of two signals. Thus, USHR/P is a 1+1 protection scheme.

BSHR is either two- (BSHR/2) or four-fiber line protecion switched (BSHR/4). In BSHR/2, half of the capacity on each ring is reserved for protection. When a failure occurs, the nodes adjacent to the failed site will loop the affected traffic using the reserved capacity on both rings. In BSHR/4, two fibers are dedicated as working fibers and another two fibers are dedicated

as protection fibers. Loopback mechanism is used to switch the affected traffic to protection fibers after a failure.

1.3.4 Protection Schemes in WDM networks

WDM Ring Network Protection According to International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Recommendation G.872, the optical layer consists three sub-layers: *optical channel (OCh) sub-layer*, *optical multiplex section (OMS) sub-layer*, and *optical transmission section sub-layer* [6]. The protection and restoration can be performed at either of first two sub-layers. In OCh sub-layer protection, the protected entity is the lightpath, so that OCh protection is also called path protection. In protection schemes performed at OMS sub-layer, the protected entity is the multiplex of WDM channels transmitted on a fiber. This is called link protection, because the recovery regards all the lightpaths that traverse the link as a group and switch them as a group.

WDM technology was used to upgrade the existing optical networks initially. WDM ring can be considered historically the second stage in the optical architecture evolution (the first being point-to-point) and environment in which WDM protection techniques were standardized [5].

In OCh dedicated protection ring scheme, the traffic flows in opposite directions on two fibers. Two counter-direction lightpaths are formed around the ring. The source node splits the signal in two identical copies that are transmitted on these two lightpaths. The receiver node selects the signal with better quality. This architecture is known as WDM self-healing ring. The recovery is very fast due to the factor that no optical switching has to be reconfigured and no signaling is required. But it uses exactly 50% of the installed physical resources for protection.

There are two standardized link protection schemes in OMS sub-layer: Shared protection ring (OMS-SPRing) for two- and four-fiber ring topology, which are similar to BSHR/2 and BSHR/4 in SONET/SDH ring networks. The difference is that in WDM rings, protection switching is carried out by 2 x 2 optical switches with large optical bandwidth. The optical

switch is able to switch the multiplex of WDM channels from one fiber to another. Switching is very fast, in the range of microseconds, and uses opto-mechanical technology. both of the OMS protection schemes also use 50% of the installed capacity resources.

WDM Mesh Network Protection Historically, Backbone networks have been interconnections of stacked rings. Due to the inefficiency and poor scalability of ring networks, backbone networks are expected to migrate to the mesh networks. The main reason is the development and maturity of optical crossconnects (OXC). Survivable design in mesh network is more complex than in ring networks, because there are multiple routes that can be used for recovery in mesh networks. A lightpath that is used to carry the traffic under normal condition is called a primary or a working path. A lightpath that is reserved for protection is called a backup or a protection lightpath. Protection schemes in mesh networks can be broadly classified as either link-based or path-based, as shown in Figure 1.3.

In link-based protection (also called loopback protection), backup paths (the routes can be different for different wavelengths) between the two end nodes of each link that is used by some primary paths are pre-computed. Upon the failure of a link, the working connections on the link are switched by the two end nodes of the link to their corresponding backup lightpaths. Thus, a link-based method employs local detouring, and the traffic is rerouted around the failed link.

In path-based protection, a pair of link-disjoint lightpaths are established between the source and destination nodes of each connection request. One lightpath is the primary or the working path, which is used to carry the traffic under normal condition. Another lightpath is the backup path, which is reserved for protection. When a link failure occurs, the source node of each affected lightpath switches the traffic to its backup path. A path-based method employs end-to-end detouring, and the traffic is rerouted by the source node of affected lightpath.

The link- and path-based protection schemes can be either dedicated or shared. Backup multiplexing refers to the technique that allows two or more backup lightpaths to share channelz if the corresponding primary lightpaths do not fail simultaneously. Sharing leads to saving in spare capacity, but it also requires a more complicated management. For example, in shared-

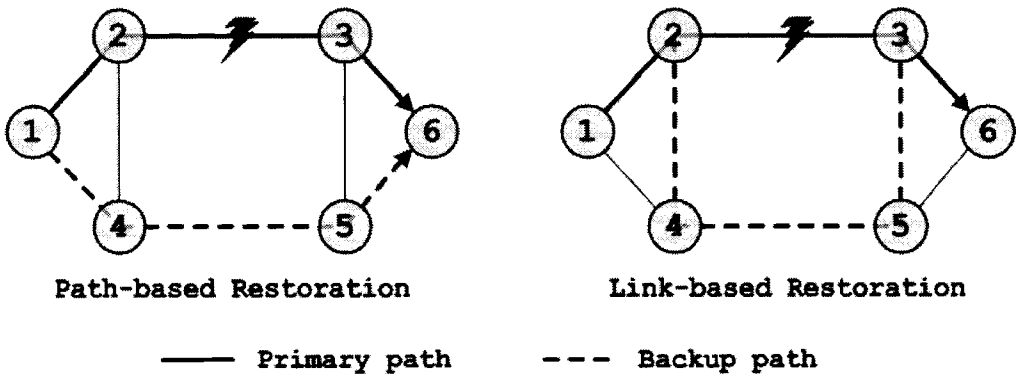

Figure 1.3 Link- and path-based protection.

path protection it is necessary to configure all the OXCs on the backup path according to which particular working lightpath needs to be recovered after a link failure occurs. This inevitably increases the recovery delay. While in dedicated protection, the OXCs on the backup lightpath can be preconfigured before the failure occurs. Only the source and destination nodes are required to perform switchings.

Link- and path-based schemes each have their respective pros and cons. In general, Shared path-based protection tends to use less total capacity than shared link-based protection, partly because the local nature of link-based methods limits the choices for alternatives. On the other hand, link-based protection tends to be faster than shared path-based protection. The reason is that in link-based protection, the failure detection and repair only involve the two end nodes of the link, whereas in path-based protection the signals must travel all the way to the source and the destination. Moreover, large signaling overhead in path-based protection can bog down the network. The backup paths in link-based protection are usually longer than in path-based protection. Another drawback for link-path protection in wavelength selective networks is that the backup path must necessarily use the same wavelength as the primary path since its working segment is retained. It is difficult if not impossible for a link-based scheme to protect against node failures.

A special type of link-based protection in mesh networks is loopback-by-ring approach,

which aims to benefit from the advantage of fast restoration of ring-like protection. Notable among these is *Double Cycle Cover* and the *p-Cycle* concept. They are both link based methods. In the double cycle cover [9], the network is represented by a directed graph. A set of cycles are embedded on the given topology. The links of the digraph are covered by two directed cycles such that each link is covered by a cycle in each direction exactly once. For planar graphs, the required set of protection cycles can be found in polynomial time, but no known polynomial-time algorithm for non-planar graphs [9]. The model uses fiber-based recovery in which working fibers are backed up by a set of protection fibers. On each link, half of the capacity are reserved for backup and the other half are used for working traffic. The traffic on fibers in one direction on a cycle is backed up by protection fibers in opposite direction on another cycle. Since the protection switches can be preconfigured, and no signaling is required upon the failure of a link, this method can achieve fast restoration. However, the capacity required for redundancy is at least 100%.

The p-cycle protection method [10] also uses cyclic layout of spare capacity to provide protection. when a link fails, only the nodes neighboring the failure need to perform real-time switching. This makes the p-cycle protection comparable to SONET/SDH line-switched rings in terms of speed of recovering from link failures. The key difference between the p-cycle protection and the ring protection is that the p-cycle protection not only protects the links on the cycle, as in the ring protection, it also protects straddling links. A straddling link is an off-cycle link whose two end nodes are both on the cycle. This important property effectively improves the capacity efficiency of p-cycles. Figure 1.4 depicts an example that illustrates p-cycle protection. In Figure 1.4 (a), A-B-C-D-E-A is a p-cycle formed using spare capacity. when an on-cycle link A-B fails, the p-cycle can provide protection as shown In Figure 1.4 (b). When a straddling link B-D fails, each p-cycle protects two working paths on the link by providing two alternate paths as shown in Figure 1.4 (c) and (d). This straddling link protection is important, because all the capacity on straddling link can be used for carrying working traffic.

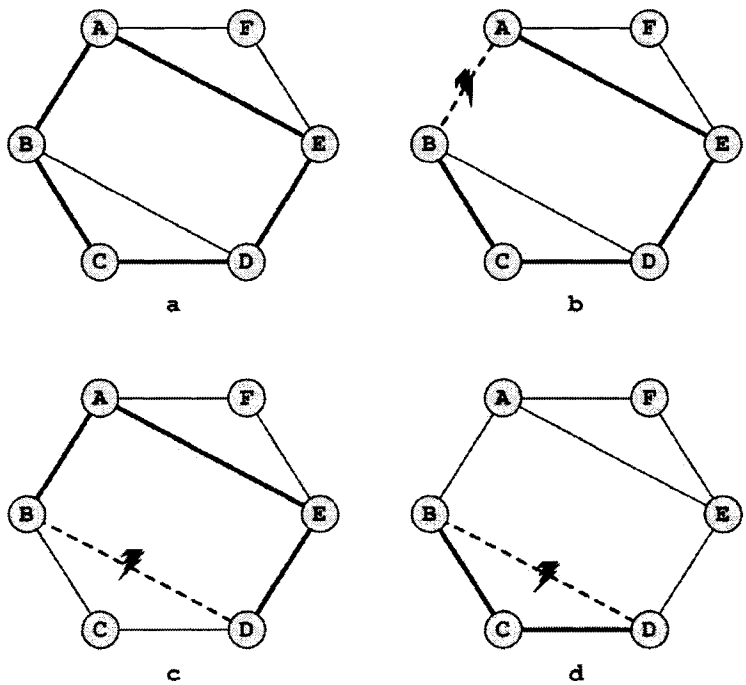

Figure 1.4 (a) An example of p-cycle. (b) protecting on-cycle links. (c) (d) protecting straddling links.

1.4 Research Issues and Contribution of the Dissertation

This dissertation addresses several important survivable design issues in WDM mesh networks.

We first consider single link failure scenarios. To achieve both high efficiency in capacity utilization and fast restoration are primary goals of survivable design in optical networks. Shared backup path protection has been shown to be efficient in terms of capacity utilization, due to the sharing of backup capacity. However, sharing of backup capacity also complicates the restoration process. As a consequence, it is believed that shared path-based protection may not be able to guarantee that the failed traffic will be restored within the 50-ms timeframe that SONET standards specify. Ring-type protection in mesh topology, on the other hand, has the potential to achieve similar restoration speed as in SONET/SDH ring networks. The p-cycle scheme is the most efficient ring-type protection method in terms of capacity utilization.

Recently, the concept of *pre-cross-connected protection* was proposed to increase the recovery speed of shared path protection [7]. One dominant factor that slows the failure recovery of shared path (or link) protection method is that the backup lightpath can't be setup at the time of connection establishment, due to backup capacity sharing. In the pre-cross-connected protection concept, the sharing of backup capacity is allowed with an additional constraint that the sharing does not compromise the ability of pre-configuring backup paths at the connection establishment time. In Chapter 2, we overview these protection methods and discuss their failure recovery processes. The recovery time of these schemes are compared analytically. To quantify the tradeoff between the capacity utilization and restoration speed, we formulate integer programming optimization problems for three protection methods in static traffic scenario, considering wavelength continuity constraint. We investigate the effect of network connectivity on the performance of capacity utilization of the methods by experimenting on topologies with different average nodal degrees.

Dynamically provisioning connections, i.e. lightpaths are established on demand as connection requests arrive at the network and torn down when connections are terminated is becoming more important in backbone transport network. Dynamic establishment of restorable connections using path-based and link-based protection methods have been studied extensively. Research on p-cycle method has been mostly focused on static traffic, where the traffic matrix is given and the problem is to find an optimal set of p-cycles. Survivable design for dynamic traffic using p-cycle technique has the potential to achieve both fast recovery and capacity efficiency. In Chapter 3, we develop a p-cycle based scheme to deal with dynamic traffic in WDM networks. We use a two-step approach. In first step, we find a set of p-cycles to cover the network and reserve enough capacity in p-cycles. By doing this, we provision the network built-in resources to be two parts: protection resources and resources available for accommodating the working traffic. The objective of partitioning the resources in this step is to guarantee that the capacity available for routing randomly arriving connection requests will be 100% protected by the reserved protection capacity in the p-cycles. The design also ensures that the p-cycles are preconfigured. In second step, we route the requests as they

randomly arrive one by one. We propose two routing algorithms. Compared to the shared path protection, in which a primary path and backup path is determined for each request as it arrives, the p-cycle based protection in this chapter considers the protection in the network as a whole in one step. This leads to less control signaling overhead and less dynamic state information to be maintained. Therefore, the p-cycle based design has the advantage of fast recovery, less control signaling, less dynamic state information to be maintained. To evaluate the blocking performance of proposed method, we compare it with shared backup path protection. Simulation results obtained from ten networks indicate that in high-connectivity or very low connectivity networks, the proposed p-cycle design has similar or even better performance in blocking probability, and thus is a better choice. In medium- or low-connectivity networks, the proposed p-cycle has higher blocking probability than shared path protection. It provides a tradeoff between the recovery speed and the blocking probability.

Although the failure of single component such as a link or a node is the most common failure scenario, it is possible to have multiple links fail simultaneously. The time to physically repair a fiber cut may be a few hours and a few days. It is possible for a second cut to happen before the first cut is repaired. Another possible multiple link failure scenario is that two links may be physically routed together for some distance due to the rights of way. A single backhoe accident may lead to the failure of both links [8]. In Chapter 4, we consider double-link failure scenario in which two links can fail simultaneously. We propose a path-based protection method for two-link failures in mesh optical networks. Two link-disjoint backup paths are pre-computed for each source and destination node pair and resources are reserved on the backup paths for each connection request. To reduce reserved backup capacity, backup capacity sharing without compromising the restoration guarantee must be explored. We identify the scenarios where the backup paths can share their wavelengths without violating 100% restoration guarantee (backup multiplexing). We use integer linear programming to optimize the total capacity requirement for both dedicated- and shared-path protection schemes. Numerical results indicate that, backup multiplexing significantly improves the efficiency of total capacity utilization.

The recently proposed *light trail* architecture offers a promising candidate for carrying IP

centric traffic over optical networks. The survivable design is a critical part of the integral process of network design and operation. The restoration methods for lightpath protection cannot be applied to light trail architecture because of the important difference that the intermediate nodes on light trail can also access the trail. In Chapter 5, We propose and compare two protection schemes, namely *connection based protection* and *link based protection*, that can achieve 100% protection against single link failure. The survivable light trail design problem using connection based protection model is solved using a two-step approach. The numerical results show that the design achieves high wavelength utilization as well as 100% protection against single link failure.

Conclusions are presented in Chapter 6.

CHAPTER 2. Comparison of Protection Mechanisms: Capacity Efficiency and Recovery Time

Survivability is an important issue in the design and operation of WDM optical networks. Preplanned protection is the primary mechanism used to deal with a failure because it can provide fast and guaranteed recovery. In contrast, dynamic restoration in which the alternate routes and resources are dynamically searched after a failure is slow and does not guarantee the success of recovery. In preplanned protection, the spare capacity needs to be reserved at the time of connection establishment. Thus, the efficient capacity utilization is an important aspect in survivable designs. Fast recovery, which leads to short "down time" and less data and revenue losses, is another major goal to be pursued.

It has long been believed that Shared path-based protection has the advantage of using capacity efficiently, whereas link-based protection tends to be faster than path-based schemes in recovery. The p-cycle scheme is a special link-based protection method, which aims to achieve ring like recovery speed and mesh-like capacity-efficiency [10]. The concept of pre-cross-connected protection captures the fact that major contribution to the fast recovery of ring-like protection is the ability of pre-configuring the backup path so that only two real time switchings are needed [7]. Adapting this concept in shared path-based protection can significantly increase the restoration speed of path-based protection.

In this chapter, we compare the performance of these protection methods in terms of recovery time and capacity efficiency in the context of WDM networks. Although the capacity performance of both shared backup path protection and p-cycle protection has been studied extensively for different network instances, there has been no direct comparison of the capacity performance of these schemes considering wavelength continuity constraint. We also study the

effect of network topology, particularly the average connectivity of the network topology, on the capacity performance of different schemes. The remainder of the chapter is organized as follows. In Section 2.1, we overview these protection methods and discuss the pros and cons. The recovery time of these protection methods are also compared analytically in this section. The capacity optimization problem is formulated for these protection schemes in Section 2.2. Section 2.3 presents the numerical results and discussion. Section 2.4 summarize this chapter.

2.1 Overview of Protection Schemes

A link failure recovery process using protection usually consists of following steps:

1. A link failure occurrence is detected.

2. The information about the failure is propagated to the nodes triggering protection switching actions.

3. Backup paths are set up. This includes the signaling and configuring the crossconnects on the backup paths. The backup routes are precomputed and backup resources are reserved in advance.

4. The affected services are switched from the failed primary paths to the corresponding backup paths.

Step 2 and 3 are the steps that result in differences in recovery time for different protection schemes. In the following, we describe three protection schemes, i.e shared path protection, p-cycle protection, and pre-cross-connected protection and compare their recovery speed.

2.1.1 Shared Path Protection

In Shared path protection, a pair of link-disjoint paths between the end nodes of a connection request are pre-computed. The connection is established on the primary path, and a wavelength is reserved on the backup path for protection. The reserved backup wavelength is not necessarily same as the wavelength used on the primary path. Assume there is only one

link failure at any instant of time, if the two primary paths are link-disjoint, the corresponding backup paths can share their backup capacity on their common links to save the backup capacity. As a result, backup channels are multiplexed among different failure scenarios that will not occur simultaneously. This backup multiplexing provides significant saving in backup capacity, but it also leads to complicated recovery process. The recovery process of shared path protection was illustrated and analysis of restoration time was given in [11, 12]. Upon detecting a link failure (Assume a link failure is detected by the nodes adjacent to the link), the end nodes of the failed link send *link-failure* message to the source and destination nodes of the each effected connection. Then, the source node of an effected connection sends a setup message to the destination node along the backup route (which is pre-determined) and configures the cross-connects at each intermediate node on the backup route. The destination node, upon receiving the setup message, sends a confirm message back to the source node. The source node switched the connection from failed primary path to the backup path after receiving the confirm message and completes the recovery.

The following notation are used in calculating the recovery time.

- F: time to detect a link failure by the nodes adjacent to the link.
- D: Message processing time at a node.
- P: The propagation delay on each fiber. The transmission time for the signaling messages can be neglected compared to the propagation delay.
- C: The time to configure and test a cross-connect.
- h_s: The number of hops from the node adjacent to the failed link to the source node of the connection.
- h_b: The number of hops in the backup route from the source node to the destination node.

Assuming that in-band signaling is used, and each node needs to cross-connect itself before it can pass the message on to the next node. The total recovery time for shared path protection

can be approximately calculated by

$$F + P \times h_s + (h_s + 1) \times D + h_b \times C + 2 \times h_b \times P + 2 \times (h_b + 1) \times D \tag{2.1}$$

2.1.2 The p-cycle Protection

The p-cycle protection method [10] uses cyclic layout of spare capacity to provide protection. The key difference between the p-cycle protection and the ring protection is that the p-cycle protection not only protects the links on the cycle, as in the ring protection, it also protects straddling links. A straddling link is an off-cycle link whose two end nodes are both on the cycle. The p-cycle protection schemes is a special type of shared link protection. In general shared link protection, the cross-connects in backup route cannot be pre-configured due to the backup resources sharing and a signaling process between two end nodes of the link is needed after a link is failed. This is not the case in p-cycle protection. In p-cycle protection, cyclic form of backup capacity enables the ring-type protection, i.e. only two end node of the link need to switch the working traffic to backup route, in which cross-connects are pre-configured. No signaling process is needed between two end nodes of the failed link. Therefore, the recovery time of p-cycle protection can be approximately calculated by

$$F + C \tag{2.2}$$

Comparing Equation 2.1 to Equation 2.2, there are two factors that lead to fast recovery of p-cycle protection: the time for propagating and processing signaling messages and the time for configuring the cross-connects in the backup route are not needed in p-cycle protection. The time to configure the cross-connects in the backup route is the dominant factor, as C is at least in the order of mini-seconds, and P and D are probably in the order of hundred micro-seconds.

Although p-cycle protection has the potential to achieve restoration speed of ring protection, it is a link-based scheme and it has the inherent limitations of link-based schemes in mesh protection. One drawback for link based schemes in the WDM mesh networks without wavelength conversion is that a backup path for a link j must necessarily use the same wavelength

used in the primary path that passes thought link j since the working segments of the primary path is retained. This complicates the problem of routing and wavelength assignment in link-based protection. Another drawback is that it is difficult if not impossible for a link-based scheme to protect against node failure.

2.1.3 Pre-Cross-Connected Protection

The dominant factor in the recovery time of shared path (or link) protection is the time to configure the cross-connects in the backup route after a link failure occurs. On the other hand, in p-cycle protection, the cross-connects in the backup route are configured before the link failure occurs. A concept of configuring the crossconnects in the backup routes before a link failure occurs in shared path-based protection was proposed by T. Y. Chow et al. in [7]. An important observation is that, although the ability of pre-cross-connecting backup paths in p-cycle protection is due to the cyclic layout of spare capacity, the converse is not true. That is, ring or cycle type protection is not the necessary condition for achieving pre-cross-connecting backup paths before a failure occurs [7]. It is possible to achieve this in path-based protection. Figure 2.1 (a) and (b) illustrate the scenarios.

In Figure 2.1 (a), general shared path protection is used. Suppose there are primary paths $1 \rightarrow 2 \rightarrow 4$ and $5 \rightarrow 4$, and corresponding backup paths $1 \rightarrow 3 \rightarrow 4$ and $5 \rightarrow 3 \rightarrow 4$. Wavelengths are shared on link $(3,4)$ for these two backup paths. If link $(1,2)$ fails, node 3 must connect link $(1,3)$ and $(3,4)$, whereas if link $(5,4)$ fails, node 3 must connect $(5,3)$ and $(3,4)$ to reroute the failed traffic. Thus the cross-connects in node 3 cannot be preconfigured. Real-time switching has to be performed after a link failure, and therefore, the restoration is slowed down.

If we employ the routing shown in Figure 2.1 (b), the above scenario can be avoided. Suppose the backup path for primary path $5 \rightarrow 4$ is $5 \rightarrow 1 \rightarrow 3 \rightarrow 4$, and wavelengths are shared on link $(1,3)$ and $(3,4)$ for the two backup paths. Then, the crossconnects in node 1 can be pre-configured to connect to node 3, and the the crossconnects in node 3 can be pre-configured to connect to node 4 before a link failure occurs. Real-time switching in nodes

3 and 4 are not needed.

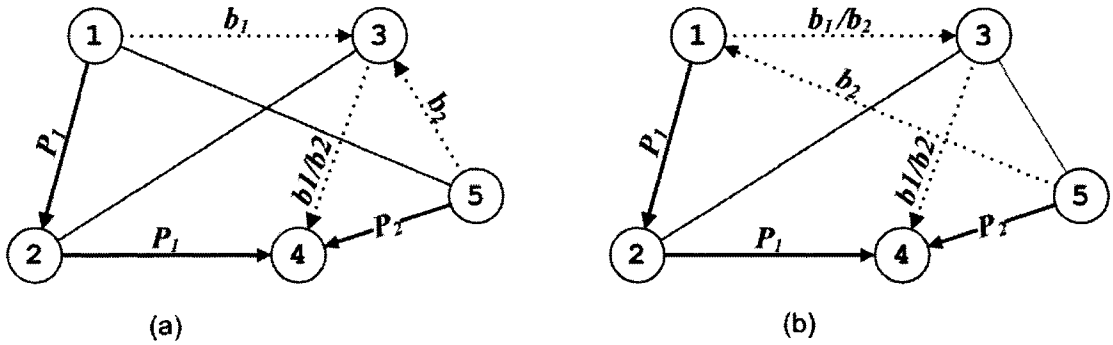

Figure 2.1 Example of pre-cross-connecting the backup path.

To realize pre-cross-connecting backup path, such scenario as the node 3 in Figure 2.1 (a) must be avoided. This can be described as following constraint. Suppose link j, l and m share a common node n. If backup path b_1 uses link j and l, and backup path b_2 uses link j and m, then b_1 and b_2 cannot share the backup capacity, as illustrated in Figure 2.2.

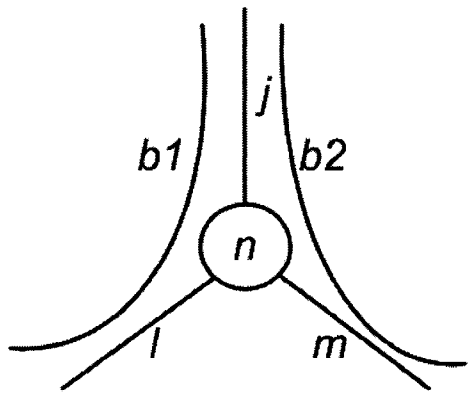

Figure 2.2 Pre-cross-connect constraint.

We call the shared path protection with this additional constraint pre-cross-connected shared path protection. Because only the source and destination nodes of a connection need to do real time switching after a link failure, the recovery time for pre-cross-connected shared

path protection is

$$F + P \times h_s + (h_s + 1) \times D + C + 2 \times h_b \times P + 2 \times (h_b + 1) \times D \tag{2.3}$$

Pre-cross-connected shared path protection is still slower than p-cycle protection in recovery, because it is path-based protection and the signaling process is still needed. It is significantly faster than general shared path protection. But the reserved backup capacity in pre-cross-connected shared path protection is expected to be more than that in general shared path protection due to the additional constraint on the sharing. In the following section, we compare the capacity performance of the three protection schemes.

2.2 Capacity Performance Comparison: Case Study

In this section, we compare the capacity utilization performance of these three protection schemes for static traffic.

2.2.1 Related Work

The problem of restorable network design for a static traffic demand has been dealt with in [11, 13, 14, 15, 16, 17]. Other works [18, 19] study dynamic scenarios. In [13], the problems of designing the restoration network for a given set of demands for wavelength-convertible networks have been considered. The problem has been formulated as an integer programming problem. The objective function is to minimize the weighted number of wavelength required. The links are weighted by capacity consumption per wavelength. The failure-independent path-based restoration is used. In [14], ILP formulations have been developed for three different protection based methods: dedicated-path protection, shared-path protection (backup multiplexing) and shared-link protection (backup multiplexing). The objective is to minimize the number of wavelength-links in a single-fiber wavelength-selective networks. In [15, 16], the various operational phases in survivable WDM networks were captured as a single ILP problem. The study also considered service disruption aspects. Spare capacity for path and span restorable networks were optimized and compared in [17]. A distributed control protocol

for dynamic-restoration-based methods has been proposed in [11]. Upon a link failure, this protocol searches for backup lightpaths for the failed lightpaths. Both the link-based and path-based restorations have been considered.

The design of p-cycle restorable network for the static traffic was formulated as an Integer Linear Programming problem in [10, 21]. First a set of all simple distinct cycles up to some upper bounded size is generated. The ILP solution identifies the optimal set of p-cycles in spare capacity of network by choosing the number of copies of each elemental cycle to be configured as p-cycles. To reduce the computation complexity, an idea of pre-selecting a subset of cycles was proposed in [22]. A subset of cycles that have "high merit" are pre-selected and then provided to an otherwise unchanged optimal solution model. The algorithm in [23] computes a set of candidate p-cycles by generating a combination of high efficiency cycles and short cycles so that the densely distributed and sparsely distributed working capacity can be efficiently protected. Straddling link algorithm (SLA) [24] generates a single p-cycle that straddles each network link if possible. A two-step algorithmic approach for the p-cycle optimization problem has been proposed in [25]. In first step, A set of candidate p-cycles is computed. In second step, one p-cycle is chosen iteratively from the candidate p-cycle set and used to reduce the unprotected working capacity until all working capacities are protected.

The joint optimization for a p-cycle design was considered in [22]. In joint optimization design, one attempts to optimize the choice of routing working connections in conjunction with the p-cycle selection so that the total capacity is minimized. Survivable designs in WDM network with or without wavelength conversion using the p-cycle concept were studied in [26]. Non-joint version optimization problem for both cases were formulated as integer linear programming problem.

2.2.2 Formulation of Capacity Optimization Problem

In the scenario of static traffic, the connection requests are given and design problem is to find an optimal routing and wavelength assignment so that the connections are established and are restorable when any single link fails. We consider 100% restoration guarantee against any

single link failure. The objective of the optimization is to minimize the total capacity used.

Network Model We assume that the network is a single-fiber mesh network and it is represented as a directed graph. There is no wavelength conversion in the network. Therefore wavelength continuity constraint applies. A set of K link-disjoint alternate routes for every source-destination pairs is pre-computed. For a network with W wavelengths, K link-disjoint alternate routes can be viewed as $K \times W$ paths, each of which is wavelength continuous. Thus, we use this wavelength continuous path as a unit (it is a lightpath if it is used to establish a connection) in the formulation to ensure the wavelength continuity. Here we choose $K = 2$. Therefore, for $1 \leq i \leq W$, path i is the path with wavelength i on the first route of a s-d pair. For $W + 1 \leq i \leq 2W$, path i is the path with wavelength i on the second route of a s-d pair.

In shared path protection, the capacity optimization problem is to choose a pair of link-disjoint paths for each connection request node pair, one of which is identified as primary path and the other as backup path. The objective function is to minimize the total capacity required.

In p-cycle protection, a set of candidate cycles is pre-computed using algorithm developed in [27]. We impose a restriction on the allowable length of p-cycles in this study. One reason is for practical purpose. The p-cycle protection is link-based approach. If long cycle is used, the lightpath after protection switching can become very long since the working segment of the primary path is also retained. Another reason is that as the number of network nodes and the network connectivity increase, the number of elemental cycles increases exponentially. In the case study, we used hop-length 6 as the maximum length limit for p-cycles. Thus, a set of candidate cycles with maximum length 6 hops is pre-computed. The joint version of capacity optimization is considered here. That is, we consider the routing for working traffic with the selection of protection cycles together. The optimization problem is to choose a primary path for each connection request, and identify a set of p-cycles so that each link on a primary path is protected by a p-cycle and total required capacity (working and backup) is minimized. The wavelength on a selected p-cycle is the same as the wavelength used by the primary path passing through the link protected by the p-cycle, as the wavelength continuity constraint is

assumed here.

Notation The following notations are used in the formulation.

- $n = 1, 2 \ldots, N$: Number assigned to each node
- $l, k = 1, 2 \ldots, L$: Number assigned to each link
- $\lambda = 1, 2 \ldots, W$: Number assigned to each wavelength
- $i, j = 1, 2 \ldots, N(N-1)$: Number assigned to s-d pair
- $K = 2$: Number of alternate routes between s-d pair
- $p, r = 1, 2, \ldots, KW$: Number assigned to a path
- (i, p) : Refers to the pth path for s-d pair i
- d_i: Demand for node pair i, in terms of number of lightpath requests
- ρ_l^n: It takes a value one if node n is an end node of link l, zero otherwise (data)

The following notations are used for path information

- $\delta^{i,p}$: It takes a value one if (i, p) is chosen as a primary path, zero otherwise (binary variable)
- $\nu^{j,r}$: It takes a value one if (j, r) is chosen as a restoration path, zero otherwise (binary variable)
- $\epsilon_l^{i,p}$: Link indicator, which takes a value one if link l is used in path (i, p), zero otherwise (data)
- $\psi_\lambda^{i,p}$: Wavelength indicator, which takes a value one if λ is used by the path (i, p), zero otherwise (data)
- $g_{l,\lambda}$: It takes a value one if wavelength λ is used by some restoration routes that traverses link l (binary variable)

- s_l: Number of wavelengths used by backup lightpaths, which pass link l (variable)
- w_l: Number of wavelengths used by primary lightpaths, which pass link l (variable)
- $I_{(i,p)(j,r)}$: It takes a value one if paths (i,p) and (j,r) share link(s), zero otherwise. If $i=j$, then $p \neq q$ (data)
- $\Pi_{(i,p)(j,r)}$: The number of shared links between paths (i,p) and (j,r) (data)

The above notations are also used in the formulation in Chapter 4. The following notations are used in formulation for p-cycle protection.

- $c = 1, 2 \ldots, P$: Number assigned to a cycle.
- ω_c^l: Link indicator, which takes a value of one if link l is on cycle c; zero otherwise (data).
- σ_c^l: Protection indicator. It takes a value of one if link l is on cycle c or is a straddling link of cycle c. It takes a value of zero otherwise (data).
- τ_c^λ: Takes a value of one if cycle c is chosen as a p-cycle in the design and uses wavelength λ , zero otherwise. (binary variable)

ILP Formulation for General Shared Path Protection The objective is to minimize the total number of wavelengths used on all the links in the network (for both the primary and backup paths).

$$Min \sum_{l=1}^{L} (w_l + s_l) \tag{2.4}$$

1. Link capacity constraint:

$$w_l + s_l \leq W \qquad 1 \leq l \leq L \tag{2.5}$$

2. Demand constraint for each node pair:

$$\sum_{p=1}^{KW} \delta^{i,p} = d_i \qquad 1 \leq i \leq N(N-1) \tag{2.6}$$

3. Primary link capacity constraint: Define the number of primary lightpaths traversing each link.

$$w_l = \sum_{i=1}^{N(N-1)} \sum_{p=1}^{KW} \delta^{i,p} \epsilon_l^{i,p} \qquad 1 \leq l \leq L \tag{2.7}$$

4. Spare capacity constraint: Definition of spare capacity required on link l.

$$s_l = \sum_{\lambda=1}^{W} g_{l,\lambda} \quad 1 \le l \le L \tag{2.8}$$

5. Primary path wavelength usage constraint: Only one primary path can use a wavelength λ on link l, no restoration path can use the same λ on link l:

$$\sum_{i=1}^{N(N-1)} \sum_{p=1}^{KW} \delta^{i,p} \epsilon_l^{i,p} \psi_\lambda^{i,p} + g_{l,\lambda} \le 1 \tag{2.9}$$
$$1 \le l \le L, 1 \le \lambda \le W$$

6. Restoration path wavelength usage constraint:

$$g_{l,\lambda} \le \sum_{i=1}^{N(N-1)} \sum_{r=1}^{KW} \nu^{i,r} \epsilon_l^{i,r} \psi_\lambda^{i,r} \tag{2.10}$$
$$1 \le l \le L, 1 \le \lambda \le W$$

$$N(N-1)KW g_{l,\lambda} \ge \sum_{i=1}^{N(N-1)} \sum_{r=1}^{KW} \nu^{i,r} \epsilon_l^{i,r} \psi_\lambda^{i,r} \tag{2.11}$$
$$1 \le l \le L, 1 \le \lambda \le W$$

7. Demand constraint for node pair i: There is one restoration route for each primary call. Let $u \in \{0,1\}$ and $v = 1 - u$:

$$\sum_{p=uW+1}^{(u+1)W} \delta^{i,p} = \sum_{r=vW+1}^{(v+1)W} \nu^{i,r} \qquad 1 \le i \le N(N-1) \tag{2.12}$$

8. Constraint for topology diversity of primary and backup paths: Primary and backup paths should be link disjoint. let $m, n \in \{0,1\}$; $s = 1 - m$; $t = 1 - n$. The primary path of a node pair can be any one of the two alternate paths for this node pair. We use m^{th} path of node pair i as primary path for node pair i, n^{th} path of node pair j as primary path of node pair j, s^{th} path of node pair i as backup path of node pair i, and t^{th} path of node pair j as backup path for node pair j.

If $I_{(i,m)(j,n)} = 1$,

$$(\nu^{i,sW+\lambda} \psi_\lambda^{i,sW+\lambda} \epsilon_l^{i,s} + \nu^{j,tW+\lambda} \psi_\lambda^{j,tW+\lambda} \epsilon_l^{j,t}) I_{(i,m)(j,n)} \le 1 \tag{2.13}$$
$$1 \le i, j \le N(N-1), 1 \le \lambda \le W, 1 \le l \le L$$

Pre-Cross-Connected Shared Path Protection Objective function and all the constraints in general shared path protection apply here. In addition, it is subject to the *pre-cross-connected protection constraint* discussed in section 2.1.3. Suppose link l, k and m share a common node n. If backup path b_1 uses link l and k, and backup path b_2 uses link l and m, then b_1 and b_2 cannot share the backup capacity on link l.

$$(\nu^{i,p}\epsilon_l^{i,p}\epsilon_k^{i,p}\psi_\lambda^{i,p} + \nu^{j,r}\epsilon_l^{j,r}\epsilon_m^{j,r}\psi_\lambda^{j,r})\rho_l^n\rho_k^n\rho_m^n \leq 1 \tag{2.14}$$

$$1 \leq i,j \leq N(N-1), 1 \leq p,r \leq KW, 1 \leq l,k,m, \leq L, 1 \leq n \leq N$$

P-Cycle Protection *Objective*: Same as Equation. 2.4.

1. *Link capacity constraint:* Same as Equation. 2.5.
2. *Demand constraint for each node pair:* Same as Equation. 2.6.
3. *Primary link capacity constraint:* Same as Equation. 2.7.
4. *Spare capacity constraint:* Definition of spare capacity required on link l.

$$s_l = \sum_{c=1}^{P}\sum_{\lambda=1}^{W}\omega_c^l\tau_c^\lambda \quad 1 \leq l \leq L \tag{2.15}$$

5. *Primary path wavelength usage constraint:* Only one primary path can use a wavelength λ on link l, no p-cycle can use the same λ on link l.

$$\sum_{i=1}^{N(N-1)}\sum_{p=1}^{KW}\delta^{i,p}\epsilon_l^{i,p}\psi_\lambda^{i,p} + \sum_{c=1}^{P}\omega_c^l\tau_c^\lambda \leq 1 \tag{2.16}$$

$$1 \leq l \leq L, 1 \leq \lambda \leq W \tag{2.17}$$

6. *Restoration guarantee constraint for link l:* There are enough p-cycles and wavelengths to recover the failure of link l.

$$\sum_{i=1}^{N(N-1)}\sum_{p=1}^{KW}\delta^{i,p}\epsilon_l^{i,p}\psi_\lambda^{i,p} \leq \sum_{c=1}^{P}\sigma_c^l\tau_c^\lambda \tag{2.18}$$

$$1 \leq l \leq L, 1 \leq \lambda \leq W \tag{2.19}$$

2.3 Results and Discussion

2.3.1 Network Instances

We compare the capacity performance of three protection schemes by experimenting on six topologies.

Figure 2.3 shows Pan-European COST239 network [28] with 11 nodes and 26 links. To study the effect of average nodal degree of a network on the performance of different schemes, three topologies are created by deleting edges from COST239 network. Instead of arbitrarily selecting edges to be deleted, we use the following process to select the edges to be deleted. We first use shortest path routing to route the requests in the traffic matrix shown in Table 2.1 one by one. The traffic matrix is obtained by dividing every entry of the traffic matrix in [28] by 2.5 Gbits/s. The demand unit in the matrix is one wavelength. Note that the final outcome of shortest path routing is not dependent on the order of routing requests, since every request is always routed on the shortest path between the source-destination node pair. After all the requests are routed, we then calculate the load on every link, and sort the links in increasing order of their link loads. The networks in Figure 2.4, 2.5 and 2.6 are created by deleting the first 5, 9 and 12 links in the sorted list, respectively. The above link selection process is based on the belief that removing the link that carries the least load would have the least impact on other links in the network. Other criteria can be used to select the links to be deleted. For example, we may choose to delete the links between the two nodes that have high connectivity.

The other two topologies that are used in experiments are 11-node 22-link NJ-LATA network, which has average nodal degree 4, and 14-node 21-link NSFNET, which has average nodal degree 3, shown in Figure 2.7 and 2.8, respectively.

2.3.2 An Example Solution

We first present an example to show the routing and wavelength assignment of three protection schemes.

Suppose there are thirteen connection requests, of which each demands one wavelength. The routing and wavelength assignment determined by ILP solution for general shared path

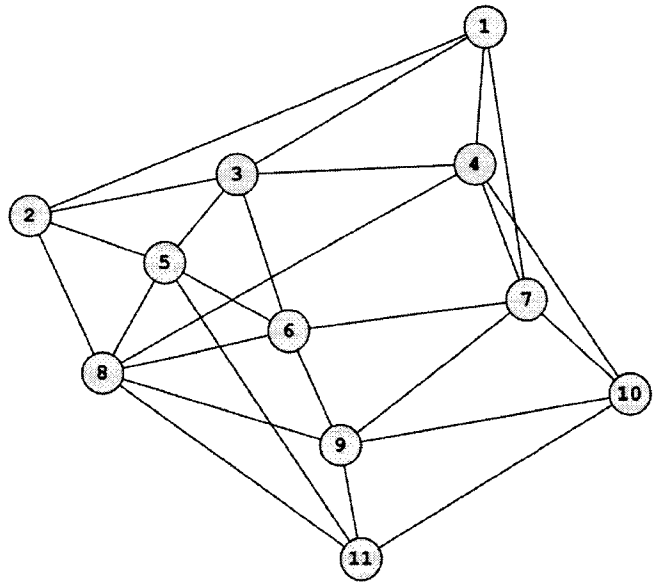

Figure 2.3 Pan-European COST 239 network.

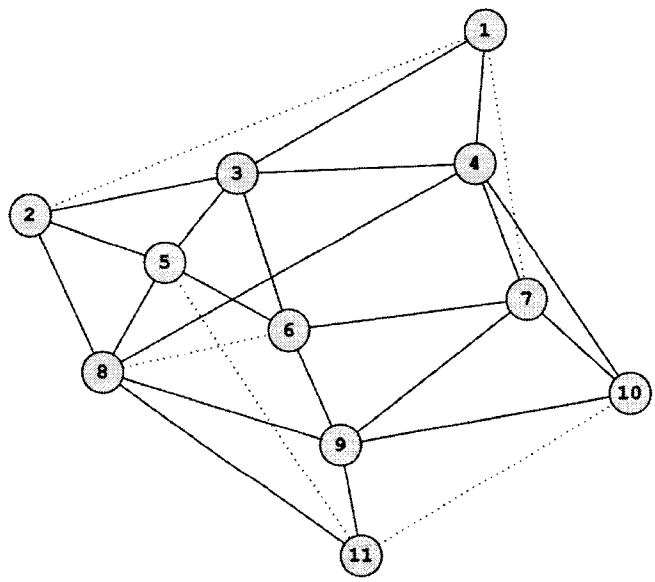

Figure 2.4 Modified Pan-European COST 239 network with 21links.

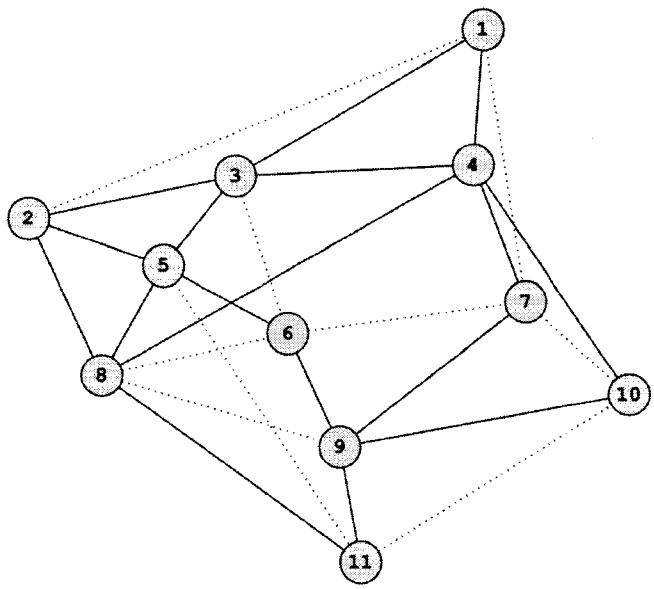

Figure 2.5 Modified Pan-European COST 239 network with 17links.

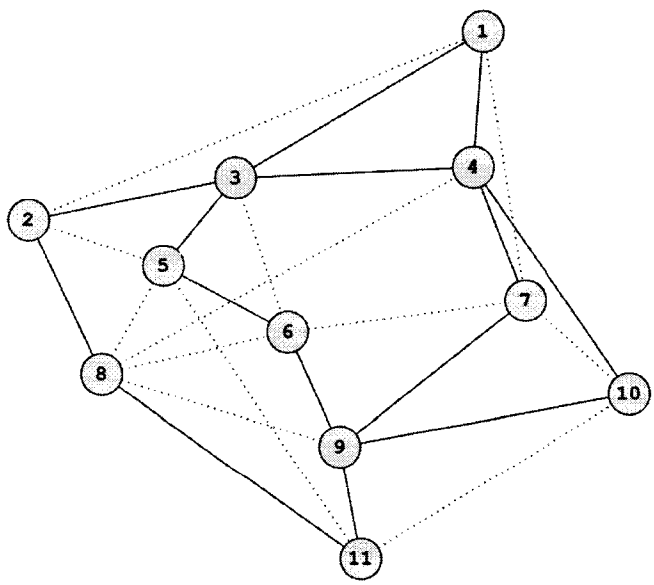

Figure 2.6 Modified Pan-European COST 239 network with 14 links.

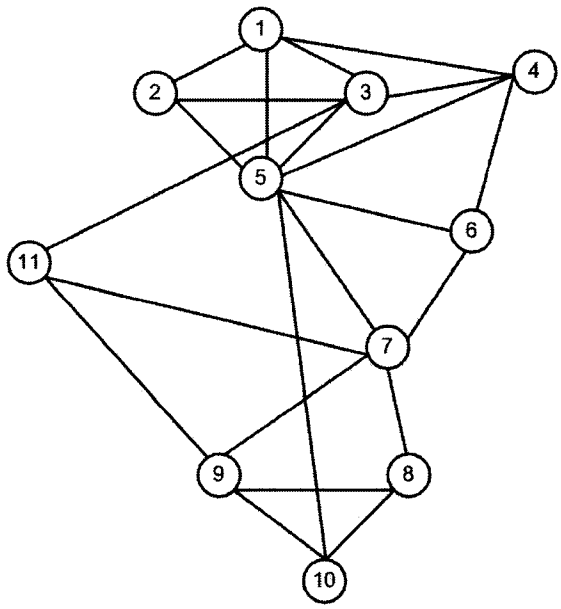

Figure 2.7 11-node 22-link NJ-LATA network.

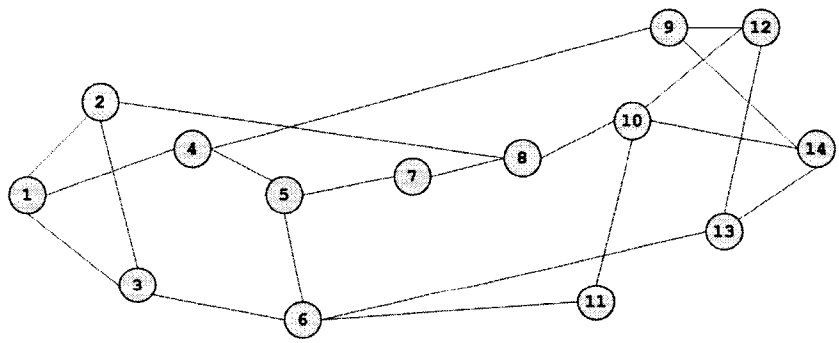

Figure 2.8 14-node 21-link NSFNET.

Table 2.1 Request matrix for cost 239 network

Node	1	2	3	4	5	6	7	8	9	10	11
1	0	1	1	3	1	1	1	1	1	1	1
2	1	0	5	8	4	1	1	10	3	2	3
3	1	5	0	8	4	1	1	5	3	1	2
4	3	8	8	0	6	2	2	11	11	9	9
5	1	4	4	6	0	1	1	6	6	1	2
6	1	1	1	2	1	0	1	1	1	1	1
7	1	1	1	2	1	1	0	1	1	1	1
8	1	10	5	11	6	1	1	0	6	2	5
9	1	3	3	11	6	1	1	6	0	3	6
10	1	2	1	9	1	1	1	2	3	0	3
11	1	3	2	9	2	1	1	5	6	3	0

protection (SBPP) and pre-cross-connected shared path protection (PRE-SBPP) are listed in Table 2.2 and 2.3. Columns 1 and 2 in the tables are source and destination nodes of each request. Columns 3 and 4 are the primary path and backup path for each request, respectively.

In the result for SBPP scheme, Wavelength $\lambda 6$ on link $(1,4)$ is shared by four backup paths: $1 \rightarrow 4$, $1 \rightarrow 4 \rightarrow 7$, $1 \rightarrow 4 \rightarrow 8 \rightarrow 11$, and $2 \rightarrow 1 \rightarrow 4 \rightarrow 10$. The cross-connect in node 4 has to be determined to connect to node 7, or node 8, or node 10 depending on which link is failed, thus it cannot be pre-configured. Due to the pre-cross-connected protection constraint, only two backup paths $1 \rightarrow 4$ and $1 \rightarrow 4 \rightarrow 7$ share wavelength $\lambda 1$ on link $(1,4)$ in PRE-SBPP. Figure 2.9 shows all the backup sharing in PRE-SBPP protection approach.

An important observation is that in PRE-SBPP, the two backup paths can share backup capacity if and only if they form a single path if they are combined.

The ILP solution identifies following five p-cycles to provide protection in p-cycle protection (PCP) approach.

1. $C_1 : 1 \rightarrow 2 \rightarrow 5 \rightarrow 8 \rightarrow 4 \rightarrow 7 \rightarrow 1$

2. C_2: $1 \rightarrow 3 \rightarrow 4 \rightarrow 1$

3. C_3: $1 \rightarrow 4 \rightarrow 7 \rightarrow 6 \rightarrow 3 \rightarrow 2 \rightarrow 1$

Table 2.2 The routing and wavelength assignment for shared path protection

Source node	Destination node	Primary path	Backup path
1	4	$1 \rightarrow 3 \rightarrow 4$ ($\lambda 8$)	$1 \rightarrow 4$ ($\lambda 6$)
1	7	$1 \rightarrow 7$ ($\lambda 7$)	$1 \rightarrow 4 \rightarrow 7$ ($\lambda 6$)
1	11	$1 \rightarrow 2 \rightarrow 5 \rightarrow 11$ ($\lambda 7$)	$1 \rightarrow 4 \rightarrow 8 \rightarrow 11$ ($\lambda 6$)
2	6	$2 \rightarrow 3 \rightarrow 6$ ($\lambda 7$)	$2 \rightarrow 5 \rightarrow 6$ ($\lambda 3$)
2	8	$2 \rightarrow 8$ ($\lambda 7$)	$2 \rightarrow 5 \rightarrow 8$ ($\lambda 3$)
2	10	$2 \rightarrow 8 \rightarrow 9 \rightarrow 10$ ($\lambda 8$)	$2 \rightarrow 1 \rightarrow 4 \rightarrow 10$ ($\lambda 6$)
3	5	$3 \rightarrow 5$ ($\lambda 7$)	$3 \rightarrow 2 \rightarrow 5$ ($\lambda 3$)
3	6	$3 \rightarrow 5 \rightarrow 6$ ($\lambda 8$)	$3 \rightarrow 6$ ($\lambda 4$)
3	7	$3 \rightarrow 4 \rightarrow 7$ ($\lambda 7$)	$3 \rightarrow 1 \rightarrow 7$ ($\lambda 1$)
4	2	$4 \rightarrow 1 \rightarrow 2$ ($\lambda 8$)	$4 \rightarrow 3 \rightarrow 2$ ($\lambda 3$)
4	11	$4 \rightarrow 10 \rightarrow 11$ ($\lambda 8$)	$4 \rightarrow 8 \rightarrow 11$ ($\lambda 6$)
5	1	$5 \rightarrow 3 \rightarrow 1$ ($\lambda 7$)	$5 \rightarrow 2 \rightarrow 1$ ($\lambda 6$)
5	3	$5 \rightarrow 3$ ($\lambda 8$)	$5 \rightarrow 2 \rightarrow 3$ ($\lambda 8$)

Table 2.3 The routing and wavelength assignment for pre-cross-connected shared path protection

Source node	Destination node	Primary path	Backup path
1	4	$1 \rightarrow 3 \rightarrow 4$ ($\lambda 8$)	$1 \rightarrow 4$ ($\lambda 1$)
1	7	$1 \rightarrow 7$ ($\lambda 8$)	$1 \rightarrow 4 \rightarrow 7$ ($\lambda 1$)
1	11	$1 \rightarrow 2 \rightarrow 5 \rightarrow 11$ ($\lambda 7$)	$1 \rightarrow 4 \rightarrow 8 \rightarrow 11$ ($\lambda 6$)
2	6	$2 \rightarrow 5 \rightarrow 6$ ($\lambda 6$)	$2 \rightarrow 3 \rightarrow 6$ ($\lambda 4$)
2	8	$2 \rightarrow 8$ ($\lambda 8$)	$2 \rightarrow 5 \rightarrow 8$ ($\lambda 3$)
2	10	$2 \rightarrow 8 \rightarrow 9 \rightarrow 10$ ($\lambda 1$)	$2 \rightarrow 1 \rightarrow 4 \rightarrow 10$ ($\lambda 8$)
3	5	$3 \rightarrow 5$ ($\lambda 8$)	$3 \rightarrow 2 \rightarrow 5$ ($\lambda 3$)
3	6	$3 \rightarrow 6$ ($\lambda 7$)	$3 \rightarrow 5 \rightarrow 6$ ($\lambda 7$)
3	7	$3 \rightarrow 1 \rightarrow 7$ ($\lambda 7$)	$3 \rightarrow 4 \rightarrow 7$ ($\lambda 7$)
4	2	$4 \rightarrow 1 \rightarrow 2$ ($\lambda 8$)	$4 \rightarrow 3 \rightarrow 2$ ($\lambda 3$)
4	11	$4 \rightarrow 10 \rightarrow 11$ ($\lambda 7$)	$4 \rightarrow 8 \rightarrow 11$ ($\lambda 6$)
5	1	$5 \rightarrow 3 \rightarrow 1$ ($\lambda 8$)	$5 \rightarrow 2 \rightarrow 1$ ($\lambda 8$)
5	3	$5 \rightarrow 3$ ($\lambda 7$)	$5 \rightarrow 2 \rightarrow 3$ ($\lambda 4$)

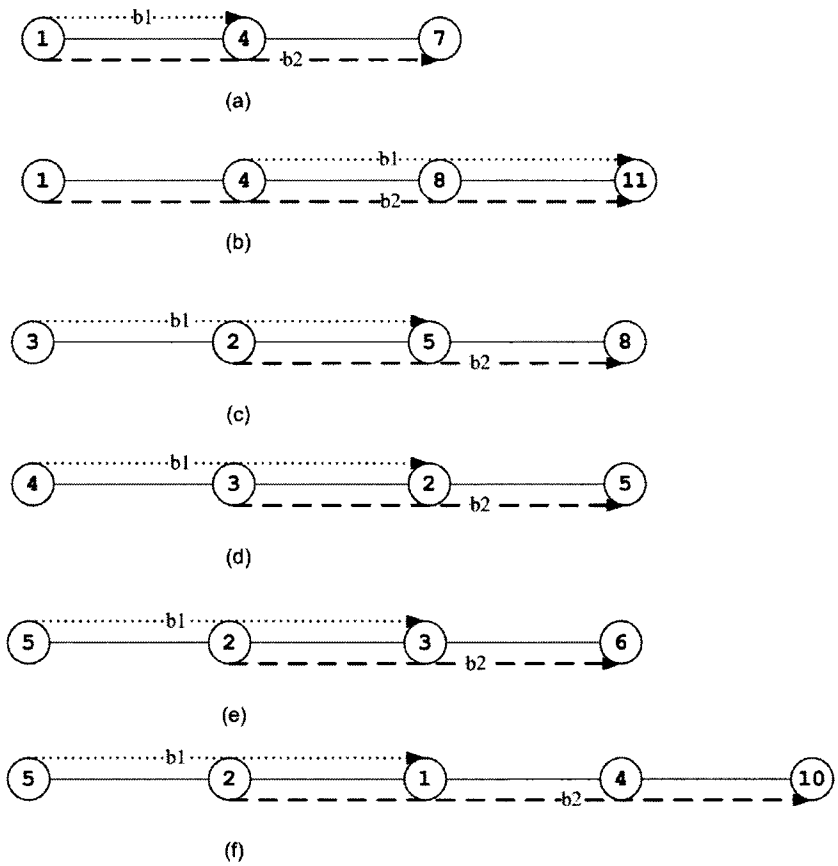

Figure 2.9 The backup sharing in PRE-SBPP scheme for the example set of connection requests.

4. C_4:1 $\rightarrow$ 7 $\rightarrow$ 6 $\rightarrow$ 5 $\rightarrow$ 2 $\rightarrow$ 3 $\rightarrow$ 1

5. C_5: 4 $\rightarrow$ 7 $\rightarrow$ 10 $\rightarrow$ 11 $\rightarrow$ 5 $\rightarrow$ 8 $\rightarrow$ 4

The routing and wavelength assignment in PCP are shown in Table 2.4. Column 3 in the table is the primary path for each request. Column 4 lists the p-cycle(s) and the wavelength(s) reserved in the p-cycle(s) that provide protection for the links on the primary path of each request. The total capacity used by SBPP, PRE-SBPP, and PCP for this example set of connection requests is 41, 43, and 49 wavelength-links, respectively.

Table 2.4 The routing and wavelength assignment for p-cycle protection

Source node	Destination node	Primary path	Protection cycle
1	4	$1 \rightarrow 4$ ($\lambda 2$)	C_1 ($\lambda 2$)
1	7	$1 \rightarrow 7$ ($\lambda 2$)	C_1 ($\lambda 2$)
1	11	$1 \rightarrow 2 \rightarrow 5 \rightarrow 11$ ($\lambda 3$)	C_4 ($\lambda 3$), C_5 ($\lambda 3$)
2	6	$2 \rightarrow 3 \rightarrow 6$ ($\lambda 5$)	C_3 ($\lambda 5$)
2	8	$2 \rightarrow 8$ ($\lambda 2$)	C_1 ($\lambda 2$)
2	10	$2 \rightarrow 1 \rightarrow 4 \rightarrow 10$ ($\lambda 3$)	C_4 ($\lambda 3$), C_2 ($\lambda 3$), C_5 ($\lambda 3$)
3	5	$3 \rightarrow 5$ ($\lambda 3$)	C_4 ($\lambda 3$)
3	6	$3 \rightarrow 6$ ($\lambda 3$)	C_4 ($\lambda 3$)
3	7	$3 \rightarrow 1 \rightarrow 7$ ($\lambda 5$)	C_3 ($\lambda 5$)
4	2	$4 \rightarrow 1 \rightarrow 2$ ($\lambda 5$)	C_3 ($\lambda 5$)
4	11	$4 \rightarrow 8 \rightarrow 11$ ($\lambda 3$)	C_5 ($\lambda 3$)
5	1	$5 \rightarrow 2 \rightarrow 1$ ($\lambda 2$)	C_1 ($\lambda 2$)
5	3	$5 \rightarrow 3$ ($\lambda 3$)	C_4 ($\lambda 3$)

2.3.3 Experiment I: Cost 239 and Traffic Matrix

The ILP formulations for three different protection schemes are solved for the traffic matrix in 2.1 and four topologies shown in Figures 2.3, 2.4, 2.5, and 2.6. The total capacity used by three different protection schemes in four topologies are presented in Table 2.5. Column two in the table is average nodal degree of four topologies. We use average nodal degree to measure the connectivity of a topology. Column three is the total capacity used by general shared path protection (SBPP) in four topologies. Column four is the total capacity used by pre-cross-connected general shared path protection (PRE-SBPP) in four topologies. Column five is the total capacity used by p-cycle protection (PCP) in four topologies. The ILP is solved using Cplex software on a 750MHz SUN machine. The optimization gap for every solution is also list in the table. Except for the solutions with optimization gap $\leq$ 0.4%, the solutions are obtained by stopping the program after running for 48 hours.

Figure 2.10 shows the plot of total capacity used by different schemes versus the average nodal degree of four test networks. As the average nodal degree increases gradually from modified cost239 network with 14 links to cost239 network with 26 links, the total capacity

Table 2.5 Total capacity used for different protection schemes in four topologies (number of wavelength-links), Optimization gap: $^1 \leq 0.4\%$, $^2 \leq 2.0\%$, $^3 \leq 3.0\%$, $^4 \leq 5.0\%$

Topology	Average node degree	General shared path protection	Pre-cross-connected shared path protection	p-cycle protection
Cost 239	4.7	816^1	948^1	794^4
Cost239 with 21 links	3.8	899^3	1039^2	908^3
Cost239 with 17 links	3.1	982^3	1108^2	1118^1
Cost239 with 14 links	2.5	1280^1	1427^3	1717^4

required for establishing restorable connections for all the requests in Table 2.1 decreases for all three protection schemes. The decline of total capacity used is due to the decline of both working and backup capacity as the network connectivity increases. There may be two factors that contribute to the improvement of capacity efficiency as the network becomes dense. First, the predetermined alternate paths become shorter as the network connectivity increases. This leads to the decrease of both working and backup capacity in all three schemes. Secondly, the opportunity for backup capacity sharing in SBPP and PRE-SBPP is likely to increase as the network connectivity increases, which leads to further decline of backup capacity in SBPP and PRE-SBPP. On the other hand, in PCP scheme, the ratio of number of straddling links versus number of on-cycle links is likely to increase as the network connectivity increases. This results in further decline of the backup capacity in PCP scheme, because more links can be protected as straddling links.

As shown in Figure 2.10, the total used capacity by SBPP and PRE-SBPP is less than that in PCP in the modified network with 14 links. SBPP still performs better than PCP in the network with 17 links, whereas PRE-SBPP uses almost same amount of total capacity as PCP. In the 21-link network and 26-link network, SBPP and PCP are comparable in terms of total used capacity, and are better than PRE-SBPP. This indicates that the improvement of capacity efficiency due to the increase of network connectivity is more dramatic in PCP scheme than in path-based protection (SBPP and PRE-SBPP).

PRE-SBPP scheme uses about 10% more capacity than SBPP in all four networks, due

to the additional pre-cross-connected protection constraint. However, the recovery speed of PRE-SBPP is expected to be significantly faster than that in SBPP, as discussed in section 2.1. Thereby, with modest increase of total capacity, PRE-SBPP can achieve fast restoration while remaining to be path-based method. It provides a tradeoff between recovery speed and capacity efficiency, especially in low-connectivity networks. Thus, it provides another option for WDM network designer in choosing protection mechanisms.

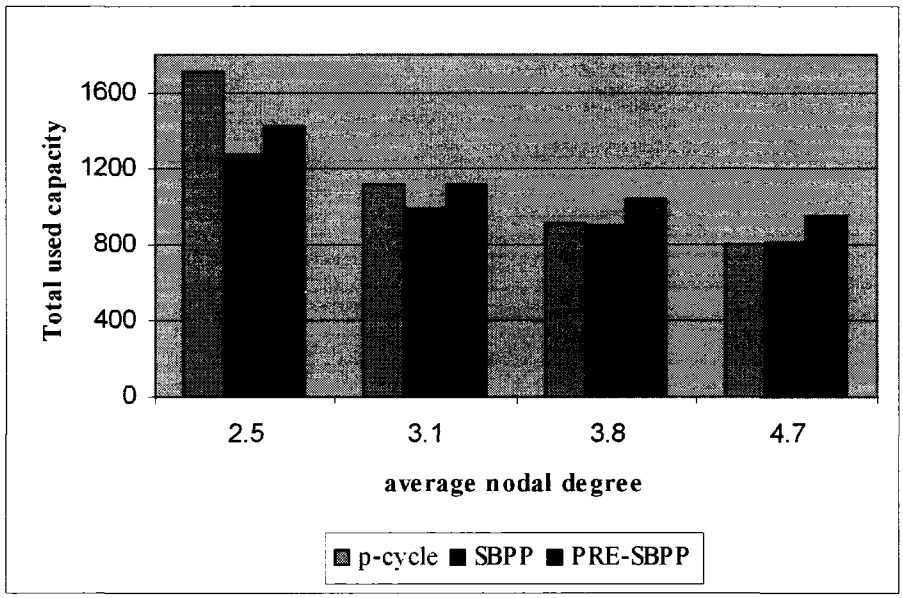

Figure 2.10 Comparison of total capacity used by three protection schemes for four topologies.

2.3.4 Experiment II: Randomly Generated Traffic Matrix

To further validate the reasoning and to study the effect of network connectivity on the capacity performance of three different protection schemes, we randomly generated two types of traffic and conducted experiments on six network topologies: Cost 239 networks with 26, 21, 17, and 14 links, NJ-LATA network, and NSFNET with 21 links. The number of requests in type II traffic is larger than that in type I traffic. There are 10 sets of requests in each of two types of traffic. The total used capacity by each of three protection schemes for each request set is obtained by solving the ILP. The average total used capacity by each protection scheme is the average value of ten request sets. The gap for all ILP solutions is 0%. Table 2.6 and 2.7 show the average total used capacity by three different schemes in six topologies for type I and type II traffic, respectively. Figure 2.11 shows the plot of average total capacity by three protection schemes versus the average nodal degree of six topologies.

Table 2.6 Average total capacity used by different protection schemes in six topologies for Type I traffic (number of wavelength-links)

Topology	Average node degree	General shared path protection	Pre-cross-connected shared path protection	p-cycle protection
Cost 239	4.7	72	74	70
NJ-LATA	4.0	78	81	83
Cost239 with 21 links	3.8	77	80	83
Cost239 with 17 links	3.1	91	97	110
NSFNET with 21 link	3.0	105	113	132
Cost239 with 14 links	2.5	106	115	136

The result in Figure 2.11 is quite in line with the result in Figure 2.10. With the increase of the network connectivity, the capacity performance of the p-cycle protection relative to SBPP and PRE-SBPP improves progressively. Cost 239 with 14 links, NSFNET with 21 links, and Cost 239 with 17links are three relatively low- connectivity networks, in which the capacity performances of SBPP are better than that of PCP; Cost 239 with 21 links, NJ-LATA network, and Cost 239 with 26 links have higher connectivity, in which PCP has comparable or even better performance with SBPP.

Table 2.7 Average total capacity used by different protection schemes in six topologies for Type II traffic (number of wavelength-links)

Topology	Average node degree	General shared path protection	Pre-cross-connected shared path protection	p-cycle protection
Cost 239	4.7	101	106	93
NJ-LATA	4.0	111	118	114
Cost239 with 21 links	3.8	110	117	112
Cost239 with 17 links	3.1	130	142	155
NSFNET with 21 link	3.0	147	162	181
Cost239 with 14 links	2.5	147	164	186

2.4 Summary

In this chapter, we conducted comparison study of three protection mechanisms, namely general shared path protection, pre-cross-connected shared path protection, and p-cycle protection for static traffic in the context of WDM networks.

We first reviewed these schemes and illustrated pre-cross-connected protection using an example. The recovery times of these protection methods were compared analytically. There are two factors that lead to fast recovery of p-cycle protection: the time for propagating and processing signaling messages and the time for configuring the cross-connects in the backup route in shared path protection are not needed in p-cycle protection. The time to configure the cross-connects in the backup route is the dominant factor. Pre-cross-connected protection eliminates the above time to configure the cross-connects in the backup route by imposing additional constraint in sharing the backup capacity. Thereby, pre-cross-connected shared path protection is significantly faster than general shared path protection. But it is still slower than p-cycle protection in recovery, because it is path-based protection and the signaling process is still needed.

We then formulated the capacity optimization problem for three schemes considering wavelength continuity constraint. We compared the capacity performance of these mechanisms and study the effect of network connectivity by experimenting on six topologies. The numeri-

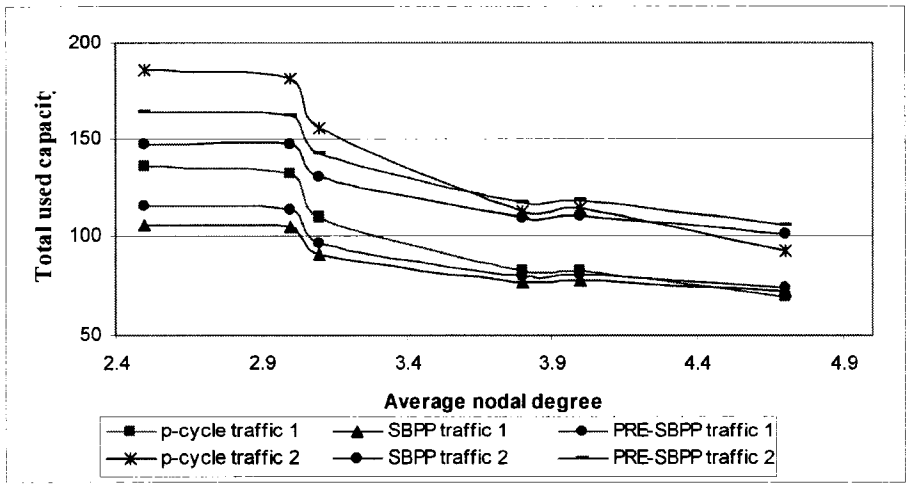

Figure 2.11 Comparison of total capacity used by three protection schemes for six topologies for random generated traffic matrices.

cal results indicate that general shared path protection and pre-cross-connected share path protection use less total capacity than p-cycle protection in low-connectivity networks, while they are comparable in high-connectivity networks. The p-cycle protection scheme appears to be a better option for protection in high-connectivity networks. Pre-cross-connected shared path protection uses more total capacity than general share backup path protection. Pre-cross-connected shared path protection can achieve fast restoration while remaining to be path-based method. It provides a tradeoff between recovery speed and capacity efficiency, especially in low-connectivity networks.

CHAPTER 3. A p-cycle Based Survivable Design and Comparison of Protection Mechanisms for Dynamic Traffic

3.1 Introduction

Dynamically provisioning connections, i.e. lightpaths are established on demand as connection requests arrive at the network and torn down when connections are terminated is becoming more important in backbone transport network. Dynamic establishment of restorable connections using path-based and link-based protection methods have been studied in the literature. Research on p-cycle method has been mostly focused on static traffic, where the traffic matrix is given and the problem is to find an optimal set of p-cycles. Survivable designs for dynamic traffic using p-cycle technique have the potential to achieve both fast recovery and capacity efficiency.

In this chapter, we consider survivable design for dynamic traffic and develop a mechanism using the p-cycle concept. We use a two-step approach. In first step, we find a set of p-cycles to cover the network and reserve enough capacity in the p-cycles. By doing this, we provision the network built-in resources to be two parts: protection resources and resources available for accommodating the working traffic. The objective of partitioning the resources in this step is to guarantee that the capacity available for routing randomly arriving connection requests will be 100% protected by the reserved protection capacity in the p-cycles. The design also ensure that the p-cycles are preconfigured. In second step, we route the requests as they randomly arrive one by one. Compared to the shared path protection, in which a primary path and backup path is determined for each request as it arrives, the p-cycle protection in this chapter considers the protection in the network as a whole in one step. This leads to less control signaling overhead and less dynamic state information to be maintained. Therefore,

the p-cycle design has the advantage of fast recovery, less control signaling, less dynamic state information to be maintained. To evaluate the blocking performance of the proposed method, we compare it with shared backup path protection. This chapter is organized as follows: The remainder of Section 3.1 reviews prior work on survivable design for dynamic traffic in WDM networks. Section 3.2 describes the survivable design model. The problem of finding an optimal set of p-cycles to cover a network topology is formulated in Section 3.3. The simulation setup is described in Section 3.6, and the results are discussed in Section 3.7. Section 3.8 summarize this chapter.

3.1.1 Related Work

The design of p-cycle restorable network for static traffic has been studied extensively. The following is a sample of the literature: [10, 21, 21, 22, 23, 24, 25, 26]. The basic approach is to generate a set of candidate cycles first. Then the solution to the capacity optimization problem identifies the optimal set of p-cycles in spare capacity of network by choosing the number of copies of each elemental cycle to be configured as a p-cycle.

The p-cycle design for establishing dynamic restorable connections has been studied in [29, 30, 31, 32]. In [29], the performance of different resilience mechanisms in protecting dynamic traffic was studied. It was concluded that there is no apparent trend showing which mechanism is the best. The performance of different schemes depends on the network topology, the network dimensioning, the load condition in the network, and the specific design of the protection method. The concept of *Protected Working Capacity Envelopes* (PWCE) was proposed in [30] to deal with dynamic traffic. The idea of PWCE is to provision over inherently protected capacity, as opposed to explicitly provision protection for every dynamically arrived connection. In PWCE, an envelope of working capacity and a separate part of spare capacity are created by a offline planning process in such a way that the envelope of working capacity is protected by the part of spare capacity. Therefore, provisioning protected service for a dynamically arrived connection is simply routing connection in the protected working envelope. The PWCE concept has the potential to offer implementation and operation advantages. In [31], performance of

Protected Working Capacity Envelopes based on p-cycle protection was studied. A dynamic restorable connection establishment scheme using p-cycle protection was proposed in [32]. For each arrived connection request, the scheme first computes a working path and then computes a set of p-cycles to protect the links on the working path.

3.2 The p-cycle Protection Model: A Two-step Approach

A p-cycle protects both the links on the cycle and straddling links of the cycle. The p-cycle protection can achieve fast recovery by preconfiguring the p-cycles. In a dynamic environment, the demands arrive at a network one by one in random manner. We do not have any information about the incoming demands in advance except maybe an estimate of distribution. To use p-cycle protection for dynamic traffic, we use a two-step approach. In first step, we consider the protection in the network as a whole. We find a set of p-cycles to cover the network and reserve capacity in the p-cycles. The objective is to partition the resources in the network into two parts: protection resources and resources available for accommodating the requests, so that the reserved protection capacity in the network is guaranteed to be enough to 100% protect the capacity available for routing working connections. We also preconfigure the p-cycles so that fast recovery after a link failure can be achieved. In second step, we route the requests as they randomly arrive one by one. The advantage of considering the protection in the network as a whole is that we do not need to worry about the protection for an individual request as it arrives. This allows us to plan the protection in advance without knowing the information about the requests, as it is the case in dynamic traffic scenario. It also reduces the control overhead, because the signaling required for providing protection for individual requests is done offline in one step.

In first step, we need to consider the following three issues.

- Selection of a set of p-cycles. The p-cycle protection is a link-based method, in which a link is protected by a cycle either as an on-cycle link or a straddling link. Since we don't have all information about the demands, we must provide protection for every link in the network, as every link may carry traffic in the future. In order to do this, we need to

select a set of cycles in such a way that every link is protected either as an on-cycle link or as a straddling link. This set of cycles will serve as p-cycles. The p-cycles also need to be preconfigured. The details of p-cycle cover problem will be discussed in section 3.3.

- Capacity allocation. To provide 100% protection against any single link failure, the capacity reserved in the p-cycles should be enough to protect any connection established using the capacity available for working connections. When an on-cycle link fails, the working traffic carried by this link will be routed using other part of the cycle. Thus, for on-cycle links, the maximum capacity that can be used for carrying working traffic is half of the initial link capacity, i.e. half of the initial link capacity on every on-cycle link needs to be reserved for protection.

- Wavelength continuity constraint. The p-cycle protection is a link-based protection method. In WDM network without wavelength conversion, a link-based method requires that the backup path for a link uses the same wavelengths as the wavelengths used by primaries that pass through the link. In Section 3.5, we discuss the "two-fiber system" that is used in the design.

To minimize the total reserved capacity, it is desired to minimize the total length of the selected p-cycles. Thus, our proposed p-cycle design for dynamic traffic scenario can be summarized in the following two steps:

1. Compute a set of cycles so that every link in the network is protected by these cycles, and the total length of all cycles is minimum. The set of cycles can be preconfigured. These cycles serve as p-cycles. For each link that is on a cycle, reserve half of the capacity for protection purpose.

2. For each arrived connection request, route the request using remaining capacity in the network.

3.2.1 Capacity Performance Metric

We define a redundancy metric to characterize the capacity utilization: network redundancy. Network redundancy (NR) is defined as ratio of total reserved capacity for protection over total available capacity for working traffic. It is determined by network topology and total available capacity when the network is built. NR is computed by

$$NR = \frac{\sum_{k=1}^{L'} 0.5 \times C_k}{\sum_{j=1}^{L} C_j - \sum_{k=1}^{L'} 0.5 \times C_k} \tag{3.1}$$

where j and k are link IDs, L is the total number of links in the network, and L' is the total number of links that are on any of the cycles that are selected as p-cycles. C_j is the initial available capacity on link j. Assume that initial available capacity on every link is same, denoted as C, then

$$NR = \frac{0.5 \times C \times L'}{L \times C - 0.5 \times C \times L'} = \frac{L'}{2 \times L - L'} \tag{3.2}$$

Case 1: no length limit for selected cycles We consider directed graphs, and we assume that the connection between any two nodes in the network is bidirectional, it is necessary that the set of selected cycles covers every node in the network at least twice. Therefore, $L' \geq 2N$, where N is the number of nodes in the network. Hence,

$$NR \geq \frac{N}{L - N} \tag{3.3}$$

where L is the number of unidirectional links in the directed graph. Equation 3.3 provide lower bounds for NR under the assumptions that every link in the network has equal length, all links are unidirectional (a bidirectional link is treated as two unidirectional links), and initial available capacity on every link is same. Using $d = L/N$, the lower bounds for network redundancy obtained by above question is in agreement with the expression $1/(d-1)$ in [33].

Case 2: length limit of K hops If we restrict that the length limit for selected cycles to K hops, multiple cycles are needed to cover every node in the network. Suppose there are r selected cycles, and the number of links on each of the selected cycles is $l_1, l_2, ..., l_r$, respectively.

We consider directed graph. Every node in the network has to be covered at least twice for directed graph. Because the graph is connected, the selected r cycles have to pass through same node(s) multiple times in order to be connected. Let m_i be the number of cycles that pass through node i. Then

$$L^{'} = l_1 + l_2 + ... + l_r = N + \sum_{i=1}^{N}(m_i - 1) \tag{3.4}$$

And

$$\sum_{i=1}^{N}(m_i - 1) \geq N - 1 + r - 1 \tag{3.5}$$

The equal sign in Equation 3.5 holds when there is no more than one common node between any two of r cycles. The reason is that when a cycle passes through a node, there is a link passes through the node, i.e., one more link is introduced. But the cycles have to be connected by some shared nodes among cycles. The scenario where total number of links in all r cycles is minimum is that there is no more than one node between any two of r cycles (a minimum case for the r-cycles to be connected).

Note $r \geq 2 \times \lceil \frac{N}{K} \rceil$. Therefore

$$L^{'} \geq N + N - 1 + 2 \times \lceil \frac{N}{K} \rceil - 1 \tag{3.6}$$

Substitute Equation 3.6 into Equation 3.2, we get that,

$$NR \geq \frac{2 \times (N + \lceil \frac{N}{K} \rceil - 1)}{2 \times L - 2 \times (N + \lceil \frac{N}{K} \rceil - 1)} \tag{3.7}$$

i.e.,

$$NR \geq \frac{N + \lceil \frac{N}{K} \rceil - 1}{L - (N + \lceil \frac{N}{K} \rceil - 1)} \tag{3.8}$$

Equation 3.8 provides lower bounds for NR when the length limit for selected cycles is K hops.

3.3 P-cycle Cover: Determining an Optimal Set of p-cycles

In the first step of design model discussed in Section 3.2, we need to find a set of p-cycles to cover the network so that every link in the network is protected either as an on-cycle link

or as a straddling link of a cycle. We consider directed graph. In directed graph, the links and cycles are unidirectional. Figure 3.1 depicts an example to illustrate the protection scenario. Suppose cycle A → D → C → B → A is a p-cycle. It can provide protection for links A →

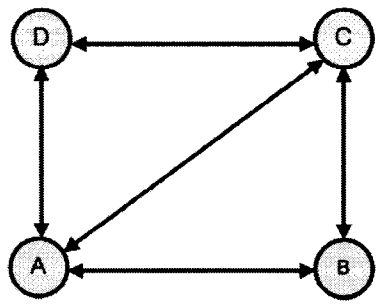

Figure 3.1 An illustrative example of p-cycle protection in directed graph

B, B → C, C → D and D → A, whose counter-direction links are on the cycle. For straddling link A → C, the p-cycle A → D → C → B → A provides only one restoration path A → D → C. Therefore, we can conclude that in directed graphs:

- A p-cycle can provide protection for a link $x \rightarrow y$ if the counter-direction link $y \rightarrow x$ is on the cycle.
- A p-cycle provides only one restoration path for its straddling links. Thus a p-cycle can only protect the working traffic on a straddling link for up to the capacity reserved on each link of the p-cycle.

In network model described in Section 3.2, we reserve half of the capacity on each on-cycle link, and reserve no capacity on straddling links. In order to provide 100% protection in a directed graph, each link l in the graph must meet one of following two constraints:

- The counter-direction link of l is on a p-cycle.
- Link l is a straddling link of two p-cycles.

The selected p-cycles need to be preconfigured in order to achieve fast recovery after a link failure. When a link fails, only the two end nodes of the failed link need to do real time

switching. The intermediate nodes along the restoration route don't need to configure the crossconnects as they are already preconfigured. To ensure this, we need to introduce a new constraint. Figure 3.2 and 3.3 illustrates the constraint. In this graph, it happens to be the case that there are no straddling links.

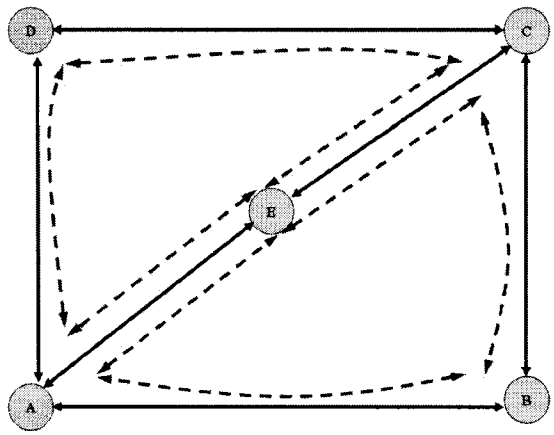

Figure 3.2 Protection scenario in which the p-cycles cannot be preconfigured.

In Figure 3.2, we use four cycles to provide protection:

- C_1: $A \rightarrow B \rightarrow C \rightarrow E \rightarrow A$
- C_2: $A \rightarrow E \rightarrow C \rightarrow B \rightarrow A$
- C_3: $A \rightarrow D \rightarrow C \rightarrow E \rightarrow A$
- C_4: $A \rightarrow E \rightarrow C \rightarrow D \rightarrow A$

Although every link can be protected, the cycles cannot be preconfigured. For example, the crossconnects in node C cannot be preconfigured. If link $A \rightarrow B$ fails, the crossconnects in node C needs to connect $E \rightarrow C$ and $C \rightarrow B$ so that cycle C_2 can be used as the protection cycle. On the other hand, if link $A \rightarrow D$ fails, the crossconnects in node C needs to connect $E \rightarrow C$ and $C \rightarrow D$ so that cycle C_4 can be used as the protection cycle.

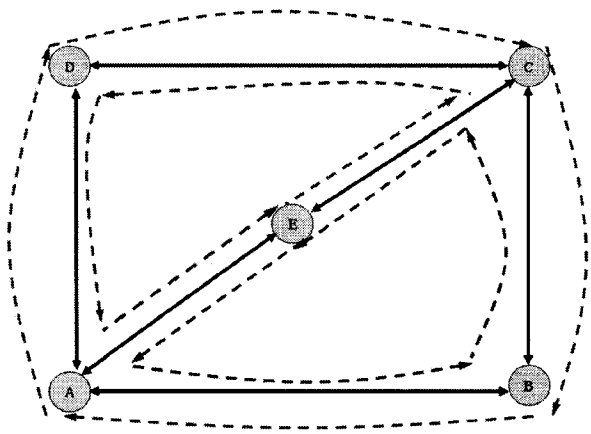

Figure 3.3 Protection scenario in which the p-cycles can be preconfigured.

In Figure 3.3, we use following three cycles to provide protection:

- C_1: $A \rightarrow B \rightarrow C \rightarrow E \rightarrow A$
- C_2: $A \rightarrow E \rightarrow C \rightarrow D \rightarrow A$
- C_3: $A \rightarrow D \rightarrow C \rightarrow B \rightarrow A$

Every link in the network is protected, and all three p-cycles can be preconfigured. An important observation is that the sharing of links such as link $E \rightarrow C$ by multiple cycles is the reason for which the cycles in Figure 3.2 cannot be preconfigured. Therefore, the sharing of a link by multiple cycles should not be allowed in the selection of p-cycles.

In summary, the problem of finding an optimal set of p-cycles in the first step of design model discussed in Section 3.2 can be defined as follows: *Given a network topology, represented as a directed graph* $G(V, E)$, *where* $|V| = N$ *and* $|E| = L$, *to identify a set of cycles with minimum total length so that for* $\forall j \in E$, j *is either covered by exactly one cycle, or is a straddling link of at least two cycles.* The problem can be formulated as Integer Linear Programming (ILP) problem. Assume the set of all simple distinct cycles in the graph is P. P is precomputed using algorithm developed in [27]. The solution of ILP then selects a set of

p-cycles.

We define the notations and formulate the problem in the following.

3.3.1 Notations

- $j = 1, 2 \ldots, P$: Number assigned to a cycle.
- L_l: The length of link l.
- ω_j^l: Link indicator, which takes a value of one if counter-directional link of link l is on cycle j; zero otherwise (data).
- σ_j^l: straddling link indicator. It takes a value of one if link l is a straddling link of cycle j, zero otherwise (data).
- δ_j: Takes a value of one if cycle j is chosen as a p-cycle in the design, zero otherwise. (binary variable)

3.3.2 ILP Formulation

1. *Objective: Minimize total length of all p-cycles. L_l is one if hop length is used.*

$$min \sum_{l=1}^{L} \sum_{j=1}^{P} \delta_j \times \omega_j^l \times L_l \tag{3.9}$$

Subject to

2. *protection constraint: Every link is either protected as an on-cycle link or as a straddling link.*

$$\sum_{j=1}^{P} \delta_j \times (\sigma_j^l + 2 \times \omega_j^l) \geq 2 \qquad \forall l \in L \tag{3.10}$$

3. *Preconfigurability constraint: No two cycles can share a link.*

$$\sum_{j=1}^{P} \delta_j \times \omega_j^l \leq 1 \qquad \forall l \in L \tag{3.11}$$

We use his formulation to identify the cycles in our simulation.

3.4 Accommodating Connections

After selecting a set of p-cycles and reserve half of the capacity on every on-cycle link for protection, we route the connections using the remaining capacity in the network as they arrive dynamically, as described in step two of two-step approach. We do not need to consider the protection when we route the connections in this step, because the accepted connections are guaranteed to be protected by the set of p-cycles identified in step one. If there is no enough capacity to route the connection, the connection is blocked.

The following two routing strategies are used, namely, $First - Shortest - Available - Path - Routing$ (FSA) and $Most - Free - Path - Routing$ (MFR). For each of two routing strategies, k shortest paths (not necessarily link-disjoint) are pre-computed for each node pair.

- *First-Shortest-Available-Path-Routing (FSA)*: When A connection arrives, the set of K shortest paths for this source-destination node pair are checked sequentially in the order of their lengths, the first path that has enough capacity is chosen to route the connection. If all K paths do not have enough capacity to route the connection, the connection is blocked.

- *Most-Free-Path-Routing (MFR)*: When a call arrives, the path that has the most free capacity among k alternate paths is chosen for routing. If there is no enough free capacity on this path, the request is blocked. The free capacity on a path is the free capacity on the link that has least free capacity among all links on the path. The free capacity on a straddling link is the capacity that is not used by existing connections. The free capacity on an on-cycle link is the capacity that is not used by existing connections and not reserved for protection, as shown in Figure 3.4. MFR aims to distribute the load evenly and reduce the blocking probability.

3.5 Wavelength Continuity Constraint

We assume that no wavelength conversion is available in the network. Therefore wavelength continuity constraint needs to hold for primary paths. The p-cycle protection is link-based

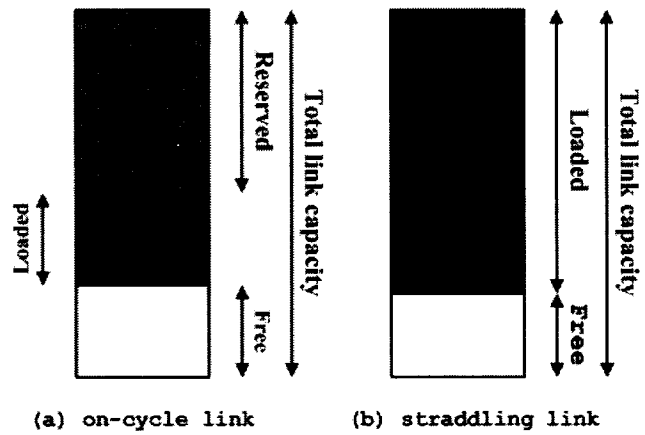

Figure 3.4 Notations on link capacity usage.

protection method. In the absence of wavelength conversion, the p-cycles have to use the same wavelength as the working path for protection. In the p-cycle design discussed above, WDM-based recovery does not yield a solution. We use Figure 3.3 to illustrate this.

In Figure 3.3, there are no straddling links. Every link is an on-cycle link. Therefore half of the capacity on each link needs to be reserved for protection. We denote the set of wavelengths that are reserved for protection on link j as SB_j, and the set of wavelengths that are available for routing working connections on link j as SP_j. For example, SB_{AE} denotes the set of wavelengths that are reserved on link $A \rightarrow E$, and SP_{AE} denotes the set of wavelengths that are available for routing working connections on link $A \rightarrow E$. Assume that initial set of wavelengths on each link in the network is the same, denoted as S, and a wavelength on a link is either reserved for protection or will be used to carry working connections in the future. Then

$$SP_j \bigcup SB_j = S, \qquad \forall j \tag{3.12}$$

$$SP_j \bigcap SP_j = \emptyset \qquad \forall j \tag{3.13}$$

Therefore,

$$SP_j = \overline{SB_j} \qquad \forall j \tag{3.14}$$

Link $A \rightarrow D$ and link $C \rightarrow B$ are in the same cycle C_3, thus

$$SB_{AD} = SB_{CB} \tag{3.15}$$

Link $B \rightarrow C$ is protected by p-cycle $C_3 : A \rightarrow D \rightarrow C \rightarrow B \rightarrow A$. Because of the wavelength continuity constraint, the set of wavelength reserved on every link of p-cycle C_3 needs to be same as SP_{BC}, i.e. $SP_{BC} = SB_{CB}$. Similarly, SP_{DA}=SB_{AD}. By 3.15, we have SP_{BC}=SP_{DA}.

By Equation 3.14, $SP_{BC} = \overline{SB_{BC}}$, and $SP_{DA} = \overline{SB_{DA}}$. Thus

$\overline{SB_{BC}}$= $\overline{SB_{DA}}$, i.e.

$$SB_{BC} = SB_{DA} \tag{3.16}$$

Link $B \rightarrow C$ and link $E \rightarrow A$ are in the same cycle C_1, thus $SB_{BC} = SB_{EA}$. Similarly, SB_{DA}= SB_{AE}. Substitute into Equation 3.16, we have

$$SB_{EA} = SB_{AE} \tag{3.17}$$

On the other hand, link $E \rightarrow A$ is protected by cycle $C_2 : A \rightarrow E \rightarrow C \rightarrow D \rightarrow A$, thus $SP_{EA} = SB_{AE}$. Equation 3.14 requires that $SP_{EA} = \overline{SB_{EA}}$, i.e. $\overline{SB_{EA}} = SB_{AE}$. This conflicts with Equation 3.17. Therefore, it proves that WDM recovery cannot meet the requirement of wavelength continuity constraint.

We use fiber-based recovery. We assume that every directional link in the network has two fibers. We reserved one fiber on each on-cycle link for protection. When a link fails, the entire traffic carried by a fiber on the link is recovered by the reserved fiber in the corresponding p-cycle. This is similar to four-fiber SHR in SONET system.

3.6 Simulation Setup

We evaluate the blocking performance of our proposed design model by carrying out simulation experiments on ten networks. Six topologies are shown in Figures 2.3, 2.4, 2.5, 2.6, 2.7, and 2.8 in Chapter 2. Other four networks are 3x3 mesh, NSFNET with 19 links, a 10-node 14

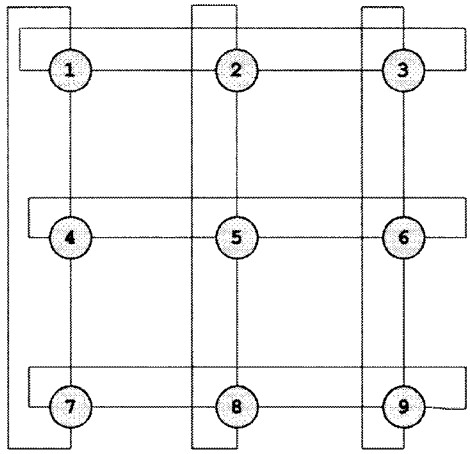

Figure 3.5 9-node 18-link 3x3 mesh network.

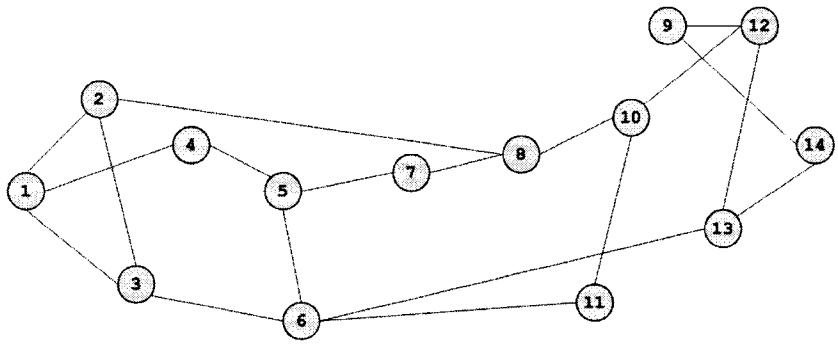

Figure 3.6 14-node 19-link NSFNET.

link network, and 10-node 12-link network, as shown in Figures 3.5, 3.6, 3.7, 3.8, respectively. These networks are chosen because they have different connectivity.

It is assumed that random requests arrive at each node according to a Poisson process with rate λ. Each request is equally likely to be destined with any of the remaining nodes. The holding time if the requests are exponentially distributed with unit mean. Hence, the Erlang load offered by a node is $\rho = \lambda/\mu = \lambda$. The capacity requirement of a request is uniformly distributed between 1 and 8 wavelengths. Initial capacity on one fiber of each link in the network is 12 wavelengths. There are two fibers on each link, therefore the initial capacity on

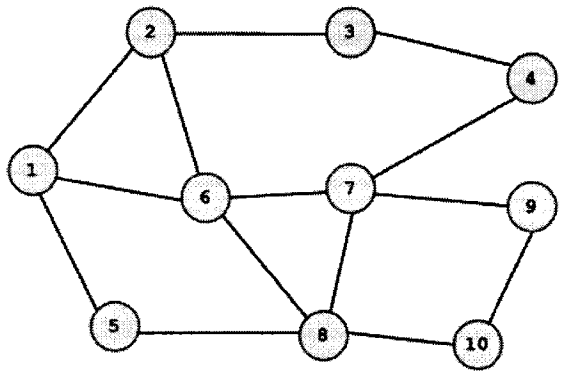

Figure 3.7 a 10-node 14-link network.

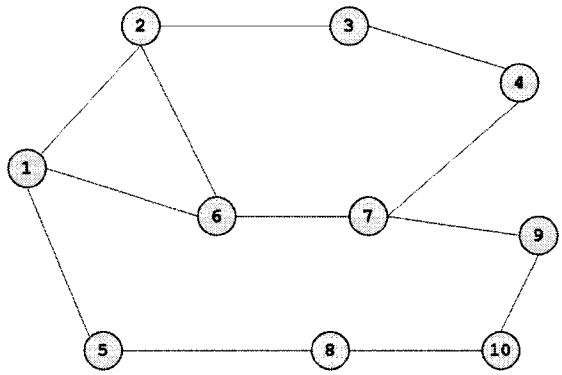

Figure 3.8 a 10-node 12-link network.

each link is 24 wavelengths.

A request is routed using routing algorithms defined in Section 3.4. The blocking probability is the ratio of number of blocked requests over total number of requests generated. For each load per node, we perform simulations in 10 rounds, with each round has 100000 random requests. An average value is taken as the blocking probability for a given load value.

3.7 Results and Discussion

3.7.1 Identified p-cycles

We consider directed graph. Each edge in the graph is treated as two unidirectional links, one in each direction. The p-cycles for each of ten networks are identified by ILP solution and are listed in the following. Different cycle length limits are used.

Cost 239 Network with no cycle length limit

1. $1 \rightarrow 3 \rightarrow 6 \rightarrow 5 \rightarrow 2 \rightarrow 8 \rightarrow 11 \rightarrow 9 \rightarrow 10 \rightarrow 7 \rightarrow 4 \rightarrow 1$

2. $1 \rightarrow 4 \rightarrow 7 \rightarrow 10 \rightarrow 9 \rightarrow 11 \rightarrow 8 \rightarrow 2 \rightarrow 5 \rightarrow 6 \rightarrow 3 \rightarrow 1$

Cost 239 Network with cycle length limit = 10hops

1. $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 10 \rightarrow 11 \rightarrow 9 \rightarrow 7 \rightarrow 1$

2. $1 \rightarrow 7 \rightarrow 4 \rightarrow 3 \rightarrow 5 \rightarrow 6 \rightarrow 9 \rightarrow 11 \rightarrow 8 \rightarrow 2 \rightarrow 1$

3. $2 \rightarrow 8 \rightarrow 11 \rightarrow 10 \rightarrow 4 \rightarrow 7 \rightarrow 9 \rightarrow 6 \rightarrow 5 \rightarrow 3 \rightarrow 2$

Cost 239 Network with cycle length limit = 7hops

1. $1 \rightarrow 2 \rightarrow 5 \rightarrow 3 \rightarrow 4 \rightarrow 10 \rightarrow 7 \rightarrow 1$

2. $1 \rightarrow 7 \rightarrow 4 \rightarrow 3 \rightarrow 6 \rightarrow 8 \rightarrow 2 \rightarrow 1$

3. $2 \rightarrow 8 \rightarrow 9 \rightarrow 6 \rightarrow 3 \rightarrow 5 \rightarrow 2$

4. $4 \rightarrow 7 \rightarrow 9 \rightarrow 8 \rightarrow 5 \rightarrow 11 \rightarrow 10 \rightarrow 4$

5. $5 \rightarrow 8 \rightarrow 6 \rightarrow 9 \rightarrow 7 \rightarrow 10 \rightarrow 11 \rightarrow 5$

NJ-LATA with no cycle length limit

1. $1 \rightarrow 4 \rightarrow 6 \rightarrow 7 \rightarrow 8 \rightarrow 10 \rightarrow 9 \rightarrow 11 \rightarrow 3 \rightarrow 2 \rightarrow 5 \rightarrow 1$

2. $1 \rightarrow 5 \rightarrow 2 \rightarrow 3 \rightarrow 11 \rightarrow 9 \rightarrow 10 \rightarrow 8 \rightarrow 7 \rightarrow 6 \rightarrow 4 \rightarrow 1$

NJ-LATA with cycle length limit = 7hops

1. $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 6 \rightarrow 7 \rightarrow 5 \rightarrow 1$

2. $1 \rightarrow 5 \rightarrow 7 \rightarrow 6 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 1$

3. $3 \rightarrow 5 \rightarrow 10 \rightarrow 8 \rightarrow 7 \rightarrow 9 \rightarrow 11 \rightarrow 3$

4. $3 \rightarrow 11 \rightarrow 9 \rightarrow 7 \rightarrow 8 \rightarrow 10 \rightarrow 5 \rightarrow 3$

3x3 Mesh with no cycle length limit

1. $1 \rightarrow 3 \rightarrow 9 \rightarrow 6 \rightarrow 4 \rightarrow 5 \rightarrow 2 \rightarrow 8 \rightarrow 7 \rightarrow 1$

2. $1 \rightarrow 7 \rightarrow 8 \rightarrow 2 \rightarrow 5 \rightarrow 4 \rightarrow 6 \rightarrow 9 \rightarrow 3 \rightarrow 1$

3x3 mesh with cycle length limit = 6hops

1. $1 \rightarrow 2 \rightarrow 8 \rightarrow 5 \rightarrow 4 \rightarrow 7 \rightarrow 1$

2. $1 \rightarrow 3 \rightarrow 6 \rightarrow 9 \rightarrow 7 \rightarrow 4 \rightarrow 1$

3. $1 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 3 \rightarrow 2 \rightarrow 1$

4. $1 \rightarrow 7 \rightarrow 9 \rightarrow 8 \rightarrow 2 \rightarrow 3 \rightarrow 1$

5. $5 \rightarrow 8 \rightarrow 9 \rightarrow 6 \rightarrow 5$

21-link Cost 239 Network with no cycle length limit

1. $1 \rightarrow 3 \rightarrow 6 \rightarrow 5 \rightarrow 2 \rightarrow 8 \rightarrow 11 \rightarrow 9 \rightarrow 10 \rightarrow 7 \rightarrow 4 \rightarrow 1$

2. $1 \rightarrow 4 \rightarrow 7 \rightarrow 10 \rightarrow 9 \rightarrow 11 \rightarrow 8 \rightarrow 2 \rightarrow 5 \rightarrow 6 \rightarrow 3 \rightarrow 1$

21-link Cost 239 Network with cycle length limit = 7hops

1. $1 \rightarrow 3 \rightarrow 6 \rightarrow 5 \rightarrow 2 \rightarrow 8 \rightarrow 4 \rightarrow 1$

2. $1 \rightarrow 4 \rightarrow 8 \rightarrow 2 \rightarrow 5 \rightarrow 6 \rightarrow 3 \rightarrow 1$

3. $4 \rightarrow 7 \rightarrow 6 \rightarrow 9 \rightarrow 10 \rightarrow 4$

4. $4 \rightarrow 10 \rightarrow 9 \rightarrow 6 \rightarrow 7 \rightarrow 4$

5. $8 \rightarrow 9 \rightarrow 11 \rightarrow 8$

6. $8 \rightarrow 11 \rightarrow 9 \rightarrow 8$

17-link Cost 239 Network with no cycle length limit

1. $1 \rightarrow 3 \rightarrow 2 \rightarrow 5 \rightarrow 6 \rightarrow 9 \rightarrow 11 \rightarrow 8 \rightarrow 4 \rightarrow 1$

2. $1 \rightarrow 4 \rightarrow 8 \rightarrow 11 \rightarrow 9 \rightarrow 6 \rightarrow 5 \rightarrow 2 \rightarrow 3 \rightarrow 1$

3. $4 \rightarrow 7 \rightarrow 9 \rightarrow 10 \rightarrow 4$

4. $4 \rightarrow 10 \rightarrow 9 \rightarrow 7 \rightarrow 4$

17-link Cost 239 Network with cycle length limit = 7hops

1. $1 \rightarrow 3 \rightarrow 5 \rightarrow 2 \rightarrow 8 \rightarrow 4 \rightarrow 1$

2. $1 \rightarrow 4 \rightarrow 8 \rightarrow 2 \rightarrow 5 \rightarrow 3 \rightarrow 1$

3. $4 \rightarrow 7 \rightarrow 9 \rightarrow 10 \rightarrow 4$

4. $4 \rightarrow 10 \rightarrow 9 \rightarrow 7 \rightarrow 4$

5. $5 \rightarrow 6 \rightarrow 9 \rightarrow 11 \rightarrow 8 \rightarrow 5$

6. $5 \rightarrow 8 \rightarrow 11 \rightarrow 9 \rightarrow 6 \rightarrow 5$

21-link NSFNET with no cycle length limit

1. $1 \rightarrow 3 \rightarrow 2 \rightarrow 8 \rightarrow 7 \rightarrow 5 \rightarrow 6 \rightarrow 11 \rightarrow 10 \rightarrow 12 \rightarrow 13 \rightarrow 14 \rightarrow 9 \rightarrow 4 \rightarrow 1$

2. $1 \rightarrow 4 \rightarrow 9 \rightarrow 14 \rightarrow 13 \rightarrow 12 \rightarrow 10 \rightarrow 11 \rightarrow 6 \rightarrow 5 \rightarrow 7 \rightarrow 8 \rightarrow 2 \rightarrow 3 \rightarrow 1$

21-link NSFNET with cycle length limit =12

1. $1 \rightarrow 2 \rightarrow 3 \rightarrow 6 \rightarrow 5 \rightarrow 7 \rightarrow 8 \rightarrow 10 \rightarrow 14 \rightarrow 9 \rightarrow 4 \rightarrow 1$

2. $1 \rightarrow 4 \rightarrow 9 \rightarrow 12 \rightarrow 10 \rightarrow 8 \rightarrow 7 \rightarrow 5 \rightarrow 6 \rightarrow 3 \rightarrow 2 \rightarrow 1$

3. $6 \rightarrow 11 \rightarrow 10 \rightarrow 12 \rightarrow 13 \rightarrow 6$

4. $6 \rightarrow 13 \rightarrow 14 \rightarrow 10 \rightarrow 11 \rightarrow 6$

5. $9 \rightarrow 14 \rightarrow 13 \rightarrow 12 \rightarrow 9$

10-node 14-link network with no cycle length limit

1. $1 \rightarrow 5 \rightarrow 8 \rightarrow 10 \rightarrow 9 \rightarrow 7 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 6 \rightarrow 1$

2. $1 \rightarrow 6 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 7 \rightarrow 9 \rightarrow 10 \rightarrow 8 \rightarrow 5 \rightarrow 1$

10-node 14-link network with cycle length limit = 7hops

1. $1 \rightarrow 2 \rightarrow 6 \rightarrow 8 \rightarrow 5 \rightarrow 1$

2. $1 \rightarrow 5 \rightarrow 8 \rightarrow 10 \rightarrow 9 \rightarrow 7 \rightarrow 6 \rightarrow 1$

3. $1 \rightarrow 6 \rightarrow 7 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 1$

4. $2 \rightarrow 3 \rightarrow 4 \rightarrow 7 \rightarrow 8 \rightarrow 6 \rightarrow 2$

5. $7 \rightarrow 9 \rightarrow 10 \rightarrow 8 \rightarrow 7$

19-link NSFNET with no cycle length limit

1. $1 \rightarrow 2 \rightarrow 3 \rightarrow 6 \rightarrow 13 \rightarrow 14 \rightarrow 9 \rightarrow 12 \rightarrow 10 \rightarrow 8 \rightarrow 7 \rightarrow 5 \rightarrow 4 \rightarrow 1$

2. $1 \rightarrow 4 \rightarrow 5 \rightarrow 7 \rightarrow 8 \rightarrow 10 \rightarrow 11 \rightarrow 6 \rightarrow 3 \rightarrow 2 \rightarrow 1$

3. $6 \rightarrow 11 \rightarrow 10 \rightarrow 12 \rightarrow 9 \rightarrow 14 \rightarrow 13 \rightarrow 6$

19-link NSFNET with cycle length limit =9

1. $1 \rightarrow 2 \rightarrow 3 \rightarrow 1$

2. $1 \rightarrow 3 \rightarrow 6 \rightarrow 5 \rightarrow 4 \rightarrow 1$

3. $2 \rightarrow 8 \rightarrow 10 \rightarrow 11 \rightarrow 6 \rightarrow 3 \rightarrow 2$

4. $1 \rightarrow 4 \rightarrow 5 \rightarrow 7 \rightarrow 8 \rightarrow 2 \rightarrow 1$

5. $5 \rightarrow 6 \rightarrow 13 \rightarrow 14 \rightarrow 9 \rightarrow 12 \rightarrow 10 \rightarrow 8 \rightarrow 7 \rightarrow 5$

6. $6 \rightarrow 11 \rightarrow 10 \rightarrow 12 \rightarrow 9 \rightarrow 14 \rightarrow 13 \rightarrow 6$

14-link Cost 239 Network with no cycle length limit

1. $1 \rightarrow 3 \rightarrow 2 \rightarrow 8 \rightarrow 11 \rightarrow 9 \rightarrow 7 \rightarrow 4 \rightarrow 1$

2. $1 \rightarrow 4 \rightarrow 10 \rightarrow 9 \rightarrow 6 \rightarrow 5 \rightarrow 3 \rightarrow 1$

3. $2 \rightarrow 3 \rightarrow 5 \rightarrow 6 \rightarrow 9 \rightarrow 11 \rightarrow 8 \rightarrow 2$

4. $4 \rightarrow 7 \rightarrow 9 \rightarrow 10 \rightarrow 4$

14-link Cost 239 Network with cycle length limit = 7hops

1. $1 \rightarrow 3 \rightarrow 5 \rightarrow 6 \rightarrow 9 \rightarrow 7 \rightarrow 4 \rightarrow 1$

2. $1 \rightarrow 4 \rightarrow 10 \rightarrow 9 \rightarrow 6 \rightarrow 5 \rightarrow 3 \rightarrow 1$

3. $2 \rightarrow 3 \rightarrow 4 \rightarrow 7 \rightarrow 9 \rightarrow 11 \rightarrow 8 \rightarrow 2$

4. $2 \rightarrow 8 \rightarrow 11 \rightarrow 9 \rightarrow 10 \rightarrow 4 \rightarrow 3 \rightarrow 2$

10-node 12-link network with no cycle length limit

1. $1 \rightarrow 5 \rightarrow 8 \rightarrow 10 \rightarrow 9 \rightarrow 7 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 6 \rightarrow 1$

2. $1 \rightarrow 6 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 7 \rightarrow 9 \rightarrow 10 \rightarrow 8 \rightarrow 5 \rightarrow 1$

10-node 12-link network with cycle length limit = 9hops

1. $1 \rightarrow 2 \rightarrow 6 \rightarrow 8 \rightarrow 5 \rightarrow 1$

2. $1 \rightarrow 5 \rightarrow 8 \rightarrow 10 \rightarrow 9 \rightarrow 7 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 1$

3. $1 \rightarrow 6 \rightarrow 7 \rightarrow 9 \rightarrow 10 \rightarrow 8 \rightarrow 5 \rightarrow 1$

4. $2 \rightarrow 3 \rightarrow 4 \rightarrow 7 \rightarrow 6 \rightarrow 2$

5. $1 \rightarrow 2 \rightarrow 6 \rightarrow 1$

3.7.2 Network Redundancy

The ten networks are categorized to four groups according to their average nodal degree. Group I is the group of high-connectivity networks, which consists of 26-link Cost239, 3x3 mesh, and NJ-LATA. Group II is the group of medium-connectivity networks, which includes 21-link Cost239, 17-link Cost239, and 21-link NSFNET. Group III is the group of low-connectivity networks, which includes 10-node 14-link network and 19-link NSFNET. Group IV is the group of very low-connectivity networks, which includes 14-link Cost239 and 10-node 12-link network. Table 3.1 shows the average nodal degree of ten networks. The ratio of straddling link is the ratio of total number of straddling links over the total number of links in the network. Network redundancy is defined in Section 3.2.1. After we identify the p-cycles for each network, we compute the ratio of straddling link and network redundancy for each network with different cycle length limit. The ratio of straddling link and the network redundancy are shown in Column 5 and 6 of Table 3.1, respectively. Figure 3.9 shows the relationship between the network redundancy for each network with no cycle length limit and average nodal degree of the network. It is observed that as the network connectivity increases, the ratio of straddling link increases, and the network redundancy decreases. This indicates that the capacity efficiency of proposed p-cycle design improves as the network connectivity increases. In Figure 3.9, 17-link Cost239 and 14-link Cost239 have unusually high network redundancy compared to the trend. This indicates there are other factors that affect the network redundancy. One factor may be that the variation of individual nodal degree in these two networks is bigger than that in other

networks. For example, in 17-link cost239 network, node 4 has nodal degree of 5, nodes 3, 5, and 8, 9 have nodal degree of 4, and all other nodes have nodal degree of 2. In contrast, in 21-link NSFNET, 12 of 14 nodes have nodal degree of 3, which is the average nodal degree of this network.

Table 3.1 Connectivity and network redundancy of ten networks

Group Index	Topology	Average nodal degree	Cycle length limit	Ratio of straddling link	NR
Group I	Cost 239 26-link	4.7	11-hop	58%	27%
			10-hop	46%	37%
			7-hop	35%	49%
	3x3 mesh	4.0	9-hop	50%	33%
			6-hop	22%	64%
	NJ-LATA	4.0	11-hop	50%	33%
			7-hop	36%	47%
Group II	Cost 239 21-link	3.8	11-hop	47%	35%
			7-hop	28%	56%
	Cost 239 17-link	3.1	11-hop	23%	62%
			7-hop	12%	79%
	NSFNET 21-link	3.0	14-hop	33%	50%
			12-hop	14%	75%
Group III	10-node 14-l network	2.8	10-hop	29%	56%
			7-hop	0%	100%
	NSFNET 19-link	2.7	14-hop	21%	65%
			9-hop	5%	90%
Group IV	Cost 239 14-link	2.5	11-hop	7%	87%
			7-hop	0%	100%
	10-node 12-l network	2.4	10-hop	4%	71%
			9-hop	0%	100%

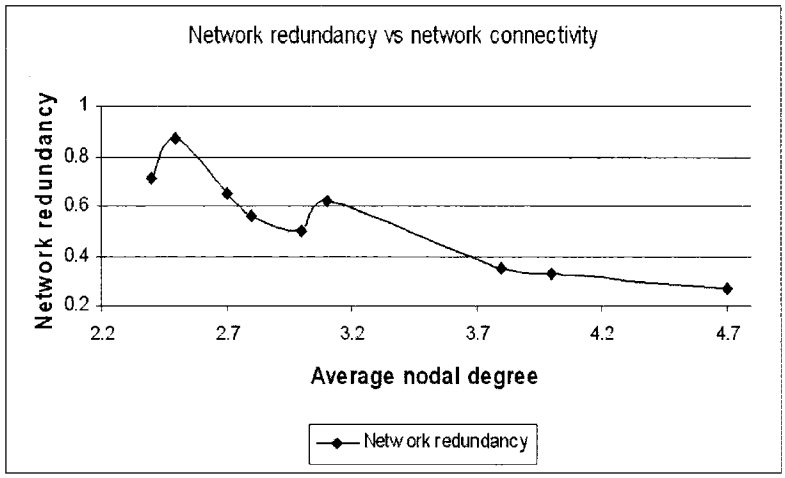

Figure 3.9 Network Redundancy versus the average nodal degree.

3.7.3 Blocking Performance

We evaluate the blocking performance of the p-cycle design by comparing with shared path protection with backup multiplexing (SBPP). Figure 3.10 to 3.19 shows the blocking probability of the p-cycle design with different cycle length limit and SBPP in ten networks.

Effect of network connectivity It is observed in Group I, i.e. high-connectivity networks (Figures 3.10, 3.11, and 3.12), the p-cycle design with no-length restriction has lower blocking probability than the backup multiplexing method. When the cycles are restricted to be shorter (maximum cycle length is 7 hops), the backup multiplexing method has lower blocking probability in NJ-LATA network, and has lower probability in Cost239 and 3x3 mesh when load per node is less than 3.5. Two methods have similar blocking probability in Cost239 and 3x3 mesh when the load per node is greater 3.5. In Group II and III, i.e. medium- and low-connectivity networks (Figures 3.13, 3.14, 3.15, 3.16, and 3.17), backup multiplexing method has lower blocking probability than the p-cycle design, except in 21-link NSFNET with no cycle

length restriction when load is greater than 3. The difference in blocking probability is within one order of magnitude when load is greater than 2.5. In Group IV, i.e. very-low-connectivity networks, the p-cycle design has similar performance in blocking probability as the backup multiplexing method, except when the load is very low.

The blocking performance of the p-cycle design improves as the network connectivity increases from Group IV to Group I. This can be explained by the change of ratio of straddling link in Table 3.1. As network connectivity increases from Group IV to Group I, the ratio of straddling link increases. Therefore more links are protected as straddling links, in which no capacity reservation is needed. The capacity in the p-cycle design are used more efficiently when the network connectivity increases, as shown by the network redundancy in column 6 of Table 3.1. This leads to the improvement of blocking performance of the p-cycle design as connectivity increases.

Effect of routing algorithms Two routing algorithms defined in Section 3.4 are used in routing working connections when they arrive randomly. Most-Free-Path-Routing (MFR) choose the path that has most free capacity to route the connection if the connection can be accepted. In First-Available-Shortest-Path-Routing (FSA), the set of K shortest paths are checked sequentially in the order of their lengths, the first available path is chosen if the connection can be accepted. Compared to FSA, MFR aims to distribute the load evenly. Figures 3.10 to 3.19 show that MFR has lower blocking probability than FSA in high-connectivity networks (Figures 3.10 and 3.12), and has similar performance in blocking probability as FSA in other networks. The reason is that in medium- or low-connectivity networks, the difference in path length for the alternate paths is bigger than that in high-connectivity networks. While MFR tries to distribute the load evenly, it tends to use longer path. The effect of using longer path on the blocking performance by MFR is more prominent in low-connectivity, and thus offset the benefit of distributing the load evenly.

Effect of p-cycle length limit As maximum length of p-cycles is restricted to be smaller, the blocking probability of the p-cycle design increases. The effect is prominent in

high-connectivity networks. If we restrict the length of p-cycles, the total length of selected p-cycles increases because the candidate set for selecting p-cycles becomes smaller. The ratio of straddling link decreases and network redundancy increases as shorter length limit is used, as shown in Table 3.1. Thus, less links are protected as straddling links when shorter cycle length limit is used. This leads to the increase of blocking probability when shorter cycle length limit is used.

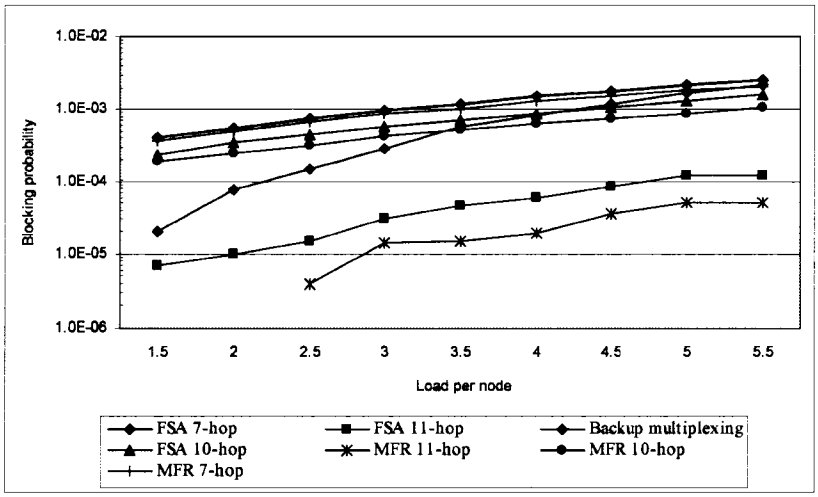

Figure 3.10 Blocking performance of 26-link Cost 239.

In summary, the proposed p-cycle based design enables faster recovery against single link failure and has less control overhead compared to shared backup path protection. In high-connectivity or very low connectivity networks, the proposed p-cycle design has similar or even better performance in blocking probability, and thus is a better choice. In medium- or low-connectivity networks, the proposed p-cycle design has higher blocking probability than shared path protection. It provides a tradeoff between the recovery speed and the blocking probability.

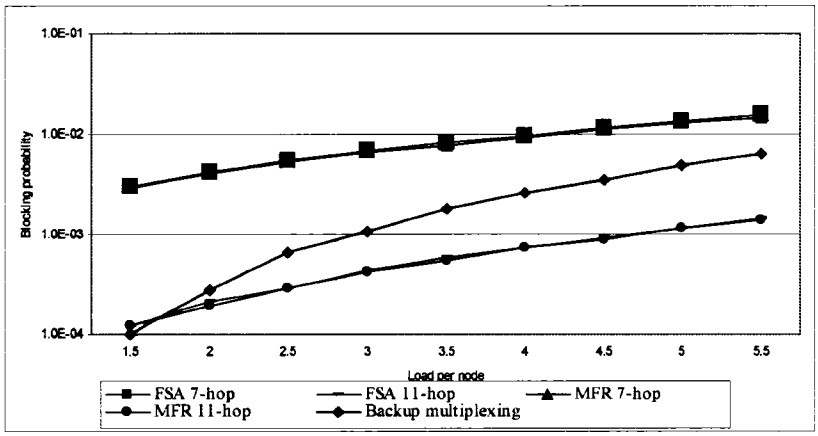

Figure 3.11 Blocking performance of NJ-LATA network.

3.8 Summary

The p-cycle concept is a type of cycle protection method in mesh network. The design goal of p-cycle protection is to retain the capacity efficiency in a mesh-restorable network, while approaching the speed of ring protection. In this chapter, we developed a p-cycle based protection method for dynamic traffic in WDM network. We use a two-step approach. In first step, we find a set p-cycles to cover the network and reserve enough capacity in p-cycles. By doing this, we provision the network built-in resources to be two parts: protection resources and resources available for accommodating the working traffic. The objective of partitioning the resources in this step is to guarantee that the capacity available for routing randomly arriving connection requests will be 100% protected by the reserved protection capacity in the p-cycles. The design also ensure that the p-cycles are preconfigured. In second step, we route the requests as they randomly arrive one by one. We propose two routing algorithms. Compared to the shared path protection, in which a primary path and backup path is determined for each request as it arrives, the p-cycle based protection in this chapter considers the protection in the network as a whole in one step. This leads to less control signaling overhead and less dynamic state information to be maintained. Therefore, the p-cycle design has the advantage of fast recovery, less control signaling, less dynamic state information to be maintained. To

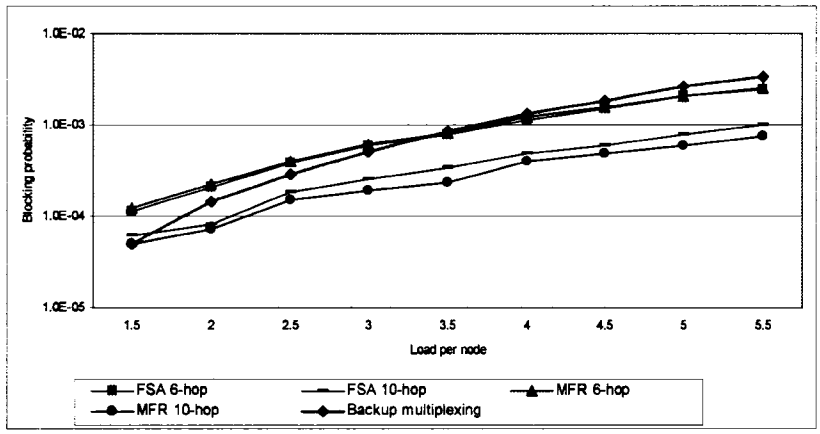

Figure 3.12 Blocking performance of 3x3 mesh.

evaluate the blocking performance of proposed method, we compare it with shared backup path protection. Simulation results indicate that in high-connectivity or very low connectivity networks, the proposed p-cycle design has similar or even better performance in blocking probability, and thus is a better choice. In medium- or low-connectivity networks, the proposed p-cycle has higher blocking probability than shared path protection. It provides a tradeoff between the recovery speed and the blocking probability.

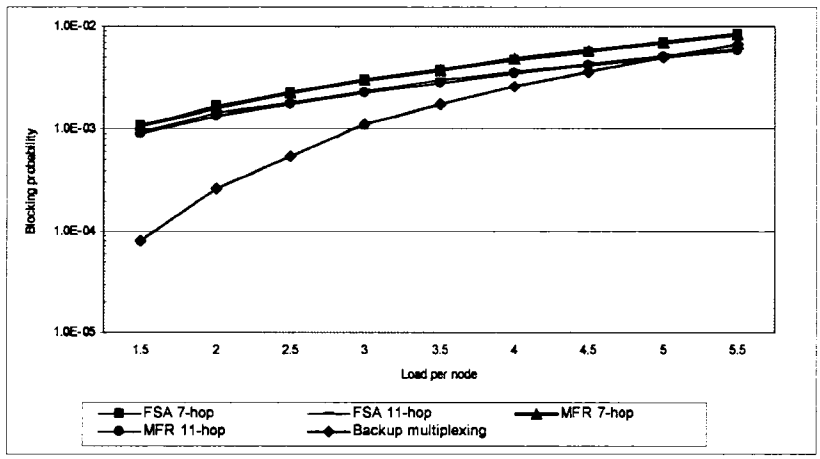

Figure 3.13 Blocking performance of 21-link cost239 network.

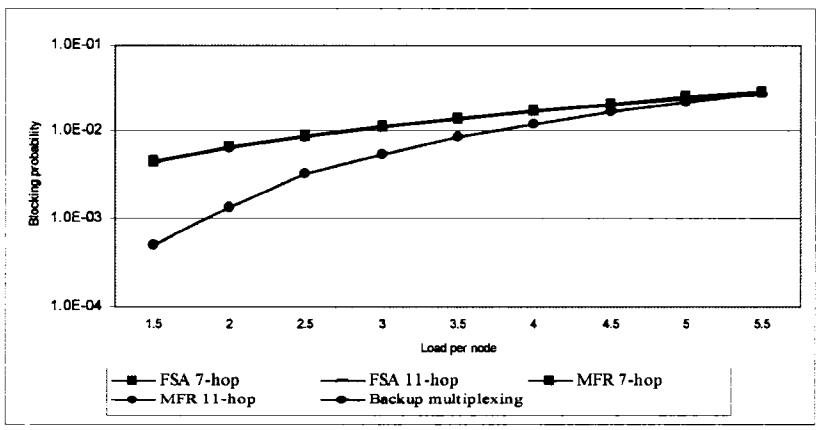

Figure 3.14 Blocking performance of 17-link cost 239 network.

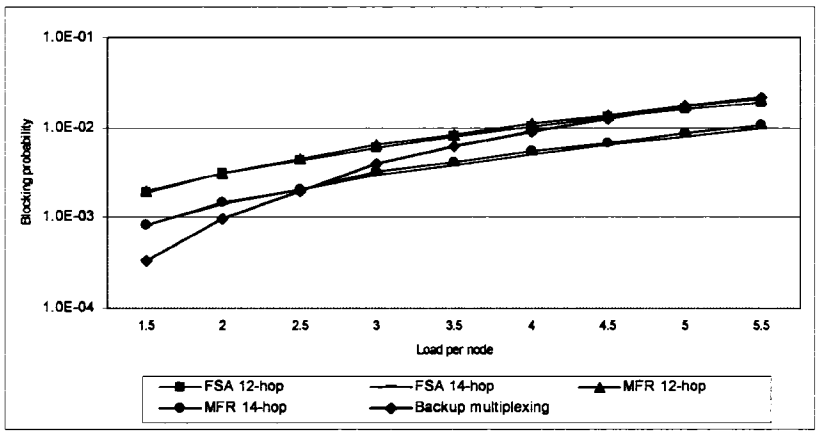

Figure 3.15 Blocking performance of 21-link NSFNET.

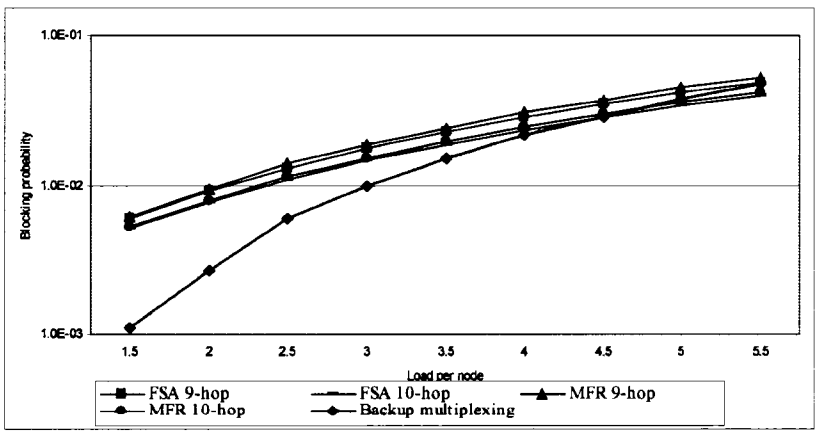

Figure 3.16 Blocking performance of 19-link NSFNET.

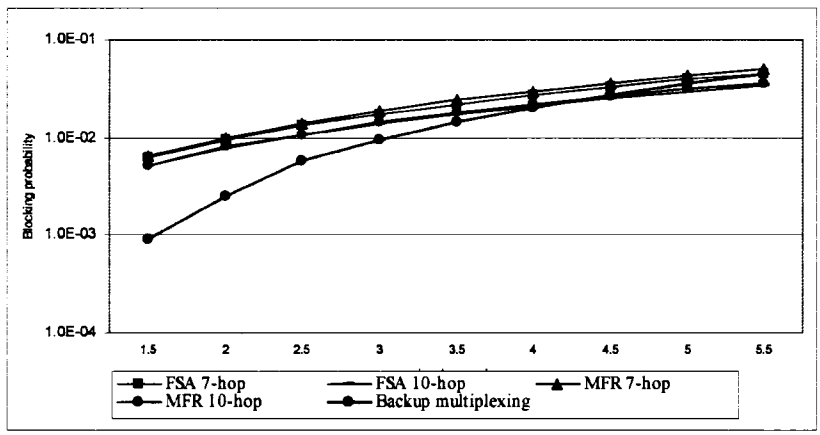

Figure 3.17 Blocking performance of 10-node 14-link network.

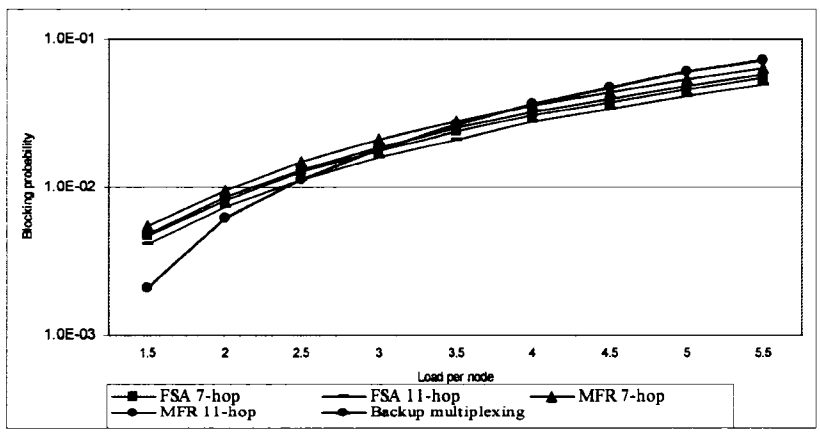

Figure 3.18 Blocking performance of 14-link cost 239 network.

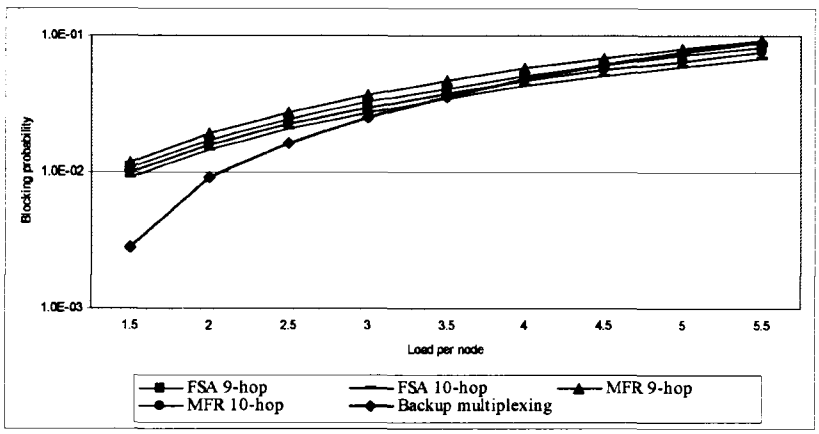

Figure 3.19 Blocking performance of 10-node 12-link network.

CHAPTER 4. Surviving Double-link Failures

WDM networks are prone to component failures, and the failures would cause catastrophic socio-economic effects due to the high volume of traffic. Although the failure of single component such as a link or a node is the most common failure scenario, it is possible to have multiple links fail simultaneously. In particular, the double link failures can happen in following scenarios:

1. The first link fails. The recovery from the failure of first link is completed within a few milliseconds to a few seconds. However, it may take a few hours to a few days to repair the failed physical link. It is certainly conceivable that a second link fails in this duration, thus causing two links to be down at the same time. Suppose the link failure is a poisson process with parameter λ and the repair times are exponentially distributed with parameter μ. Thus, the average time to failure is $1/\lambda$ and average repair time is $1/\mu$. Suppose a link fails at time $t = 0$, then the probability that a failure will occur on a link while the first repair is carried out is given by:

$$FP = \frac{\lambda}{(\lambda + \mu)}(1 - \exp(-\lambda/\mu)) \tag{4.1}$$

   For $\mu = 9\lambda$, $FP \cong .1$, which is large.

2. Two links may be physically routed together for some distance in real situations. A single backhoe accident may lead to the failure of both links.

In this chapter, we develop a path-based double link failure recovery model. The rest of the chapter is structured as follows. The remainder of this section presents previous work on surviving double link failures. Section 4.1 presents the path-based double-link failure recovery

model, and the backup multiplexing rules for identifying the scenarios where the backup wavelength sharing does not violate the 100% restoration guarantee. In Section 4.2, we develop the ILP formulation for total capacity used by dedicated-path scheme, which reserves backup capacity on every backup path, and the share-path scheme, which employs backup multiplexing. Section 4.3 presents the numerical results on capacity utilization for the two schemes and discussion. Section 4.4 summarizes this chapter.

4.0.1 Previous Work

There has been research in surviving two-link failures. Spare-channel design schemes for a self-healing network in the case of double link failures were discussed and the problem was solved using linear programming method in [35]. In [36], the two-link failures restorability of mesh networks that are designed to fully restore any single link failure was studied by experimental computational approach. The problem of minimizing the average loss caused by dual failures, while single failures are still fully survived is also studied in [37, 40]. Three link-based protection methods were presented in [38]. In [39], three different models were developed to address the design of the networks for surviving dual failures. In [41], backup multiplexing technique was developed for link-based protection methods in the case of double-link failures. The total capacity for providing 100% protection was optimized. The problem of identifying a backup path for every link that satisfies the Backup Link Mutual Exclusion (BLME) constraint was studied in [42]. BLME constraint refers to that two links may not use each other in their backup paths if they may fail simultaneously. The problem was formulated and a heuristic algorithm was developed.

4.1 Double-Link Failure Recovery Model and Backup Multiplexing

4.1.1 Double-Link Failure Recovery Model

In this section, we discuss the double-link failure recovery model adopted for our formulation. We consider a centralized pre-computed recovery model with 100% restoration guarantee against any two-link failures. The network is represented by a directed graph. For the graph

to remain connected when two edges fail, the graph must be 3-connected. We assume this is the case. To provide 100% protection against any two-link failures, two link-disjoint backup paths must be provided for every s-d pair. We assume that both links fail simultaneously (the model also works for the scenario when the second link fails during the physical repair of first failed link).

We assume that each path, primary or backup, always accommodates an OAM (operation, administration, and maintenance) channel terminated by the same s-d pair as the path [43]. When a primary path fails, an alarm indication signal is generated by the node that detects the link failure and is transferred over OAM channel. When the source receives the alarm signal in its OAM channel, it prepares to set up the first backup path. The first backup path may also be failed due to another link failure. Therefore, run time search is needed. Run time search also detects if the backup capacity on the first backup path is not available due to the sharing, in the case of shared-path scheme (detailed in the following). If the source detects the above scenarios by run time search, it will prepare to set up the second backup path; otherwise, it will use the first backup path to reroute the traffic on the primary. The source then sends messages to controller along the backup path to configure the ports accordingly. Once the backup path is setup, the communication occurs on that path. There is no restriction in our model for wavelength choice on the backup path. It may or may not be the same as the primary path.

4.1.2 A Case for Backup Multiplexing

Reserving dedicated capacity on two backup paths for every primary path would reserve excessive capacity in some situations. Figure 4.1 is an example to depict this problem. Suppose paths $1 \rightarrow 3 \rightarrow 2$ and $4 \rightarrow 5 \rightarrow 1$ are two primary paths p and r, respectively. Paths $1 \rightarrow 2$ and $1 \rightarrow 5 \rightarrow 4 \rightarrow 2$ are two backup paths for p, denoted as b_{p1}, b_{p2}. Paths $4 \rightarrow 3 \rightarrow 1$ and $4 \rightarrow 2 \rightarrow 1$ are two backup paths for r, denoted as b_{r1}, b_{r2}. The only failure scenario that could cause two primary paths to go down simultaneously is when one of links on p, and one of the links on r fail at the same time. b_{p1} and b_{r1} can be used to reroute the working traffic on p and r, respectively. Thus b_{p2} and b_{r2} will not be used at the same time for all possible

two-link failures, therefore they can share backup capacity for primary p and r on link (4,2).

On the other hand, backup capacity sharing is not always allowed if we want to provide 100% restoration guarantee against any two-link fails. Suppose the the other two primary paths p and r are $2 \rightarrow 3 \rightarrow 1$ and $4 \rightarrow 5 \rightarrow 1$, respectively. The two backup paths for p are, b_{p1}: $2 \rightarrow 1$, and b_{p2}: $2 \rightarrow 4 \rightarrow 5 \rightarrow 1$. The two backup paths for r are, b_{r1}: $4 \rightarrow 2 \rightarrow 1$, b_{r2}: $4 \rightarrow 3 \rightarrow 1$. Since p and b_{r2} have shared links, and so do r and b_{p2}, the failure of one link on p could cause b_{r2} to fail, and the failure of one link on r could cause b_{p2} to fail. If the above scenario occurs, b_{p1} and b_{r1} will be used to reroute the primary traffic on p and r, respectively. Therefore they must not share backup capacity even if they have common link (2,1).

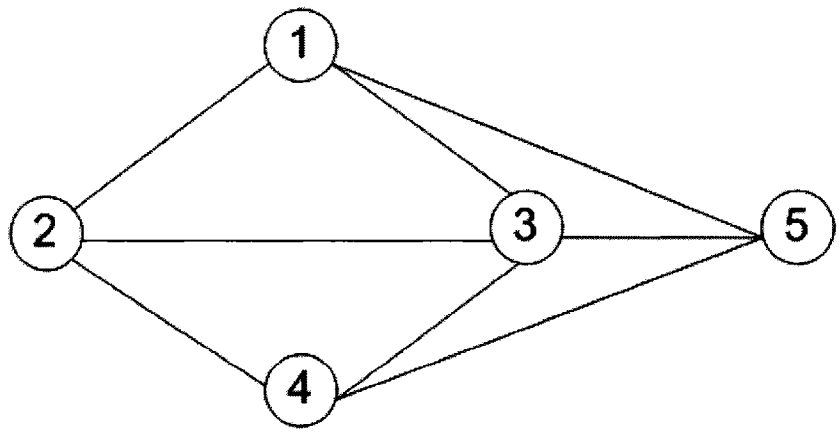

Figure 4.1 An example network.

4.1.3 Backup Multiplexing Constraints

In this section, we discuss the backup multiplexing rules for identifying the scenarios where backup paths can share backup capacity without violating the 100% restoration guarantee. Let p and r be the two primary paths, bp_1 and bp_2 be the two backup paths of p, and br_1 and br_2 be the two backup paths of r. In the following discussion, equivalent situations exist for the topology relationship between p and backup paths of r, and r and backup paths of p. For example, the following two are equivalent situations.

1. p is disjoint with br_1 and br_2, r is disjoint with bp_1 and has common link(s) with bp_2.
2. r is disjoint with bp_1 and bp_2, p is disjoint with br_1 and has common link(s) with br_2.

   For such situations, we only state one case.

4.1.3.1 Primary p and r are disjoint

The only failure scenario where two link failures cause both p and r to fail simultaneously is that one link on p and one link on r fail together. There are three possible topology relationships between p and two backup paths of r, br_1 and br_2.

1. p is disjoint with both br_1 and br_2.
2. p is disjoint with one and has shared link(s) with the other.
3. p has shared links with both br_1 and br_2.

Since br_1 and br_2 are disjoint, in the worst-case failure scenario, the failed link on p can only cause one of the backup paths br_1 and br_2 to fail. The backup path that is not failed will be used to reroute the primary traffic on r. Table 4.1 summarize the topology relationships and backup capacity sharing constraints. The following notations are used to express the topology relations and backup capacity sharing constraints.

1. b_{pi} and b_{pj}: backup paths of p; i and $j \in \{1,2\}$, $i \neq j$.
2. b_{rl} and b_{rm}: backup paths of r; m and $l \in \{1,2\}$, $m \neq l$.
3. $p \cap r = \phi$: path p and r are link-disjoint; otherwise, they have shared link(s).
4. $BC(b_{pi})$: backup capacity reserved on backup path b_{pi}.
5. $BC(b_{pi}) \wedge BC(b_{rl}) = \phi$: backup paths b_{pi} and b_{rl} must not share backup capacity on their common link(s).

4.1.3.2 Primary p and r are not link-disjoint

If the primary path p and r are not link-disjoint, one of the backup capacity constraints in the previous section is applied, depending on the primary-backup path topology relationships. In addition, the failure of the shared link of p and r will cause both p and r to go down simultaneously. The worst-case scenario is that one of the backup paths of p and one of the backup paths of r also have a common link and that link also fails, causing these two backup paths to fail at the same time. If the above failure scenario occurs, the other backup paths of p and r will be used to reroute the primary traffic on p and r, respectively. Therefore they must not share backup capacity if they have common link(s). This scenario is summarized in case 7 of Table 4.1.

Figure 4.2 illustrates the seven cases of topology relationships corresponding to Table 4.1. Here we take case (1) in Figure 4.2 as an example. In case (1), primary paths are p: $5 \rightarrow 4 \rightarrow 3 \rightarrow 9$ and $r : 1 \rightarrow 6 \rightarrow 7 \rightarrow 8 \rightarrow 9$. The backup paths for path p are $b_{p1} : 5 \rightarrow 8 \rightarrow 9$ and $b_{p2} : 5 \rightarrow 6 \rightarrow 7 \rightarrow 9$. The backup paths for path r are $b_{r1} : 1 \rightarrow 5 \rightarrow 4 \rightarrow 9$ and $b_{r2} : 1 \rightarrow 2 \rightarrow 3 \rightarrow 9$. Since path p are not link-disjoint with both b_{r1} and b_{r2}, and path r are not link-disjoint with both b_{p1} and b_{p2}, according to rule 1 in Table 4.1, no backup capacity sharing between any one of backup paths of P and any one of the backup paths of r is allowed.

Table 4.1 The topology relationships, failure scenarios and backup capacity sharing constraint

Primary paths topology relationships	Backup-primary, backup-backup topology relationships	Backup capacity sharing constraints
$p \cap r = \phi$	1. $b_{pi} \cap r \neq \phi$, $b_{rl} \cap p \neq \phi$, i and $l \in \{1,2\}$	$BC(b_{pi}) \wedge BC(b_{rl}) = \phi$
	2. $b_{pi} \cap r \neq \phi$, $b_{rl} \cap p = \phi$, $b_{rm} \cap p \neq \phi$, i, l, and $m \in \{1,2\}$, $l \neq m$	$BC(b_{pi}) \wedge BC(b_{rl}) = \phi$
	3. $b_{pi} \cap r = \phi$, $b_{pj} \cap r \neq \phi$, $b_{rl} \cap p = \phi$, $b_{rm} \cap p \neq \phi$, i, j, l, and $m \in \{1,2\}$, $i \neq j$, $l \neq m$	$BC(b_{pi}) \wedge BC(b_{rl}) = \phi$
	4. $b_{pi} \cap r = \phi$, $b_{rl} \cap p = \phi$, $b_{rm} \cap p \neq \phi$, i, l, and $m \in \{1,2\}$, $l \neq m$	$(BC(b_{p1}) \wedge BC(b_{rl}) = \phi) \|\|$ $(BC(b_{p2}) \wedge BC(b_{rl}) = \phi)$
	5. $b_{pi} \cap r = \phi$, $b_{rl} \cap p \neq \phi$, i and $l \in \{1,2\}$	$((BC(b_{p1}) \wedge BC(b_{r1}) = \phi) \|\|$ $(BC(b_{p2}) \wedge BC(b_{r1}) = \phi)) \&\&$ $((BC(b_{p1}) \wedge BC(b_{r2}) = \phi) \|\|$ $(BC(b_{p2}) \wedge BC(b_{r2}) = \phi))$
	6. $b_{pi} \cap r = \phi$, $b_{rl} \cap p = \phi$, i and $l \in \{1,2\}$	$(BC(b_{p1}) \wedge BC(b_{r1}) = \phi) \|\|$ $(BC(b_{p2}) \wedge BC(b_{r1}) = \phi) \|\|$ $(BC(b_{p1}) \wedge BC(b_{r2}) = \phi) \|\|$ $(BC(b_{p2}) \wedge BC(b_{r2}) = \phi)$
$p \cap r \neq \phi$	In addition to the above primary- and backup cases, there is one backup-backup relationship we need to consider 7. $b_{pi} \cap b_{rl} = \phi$, $i, l \in \{1,2\}$	$BC(b_{pj}) \wedge BC(b_{rm}) = \phi$, j and $m \in \{1,2\}$, $j \neq i$, $m \neq l$

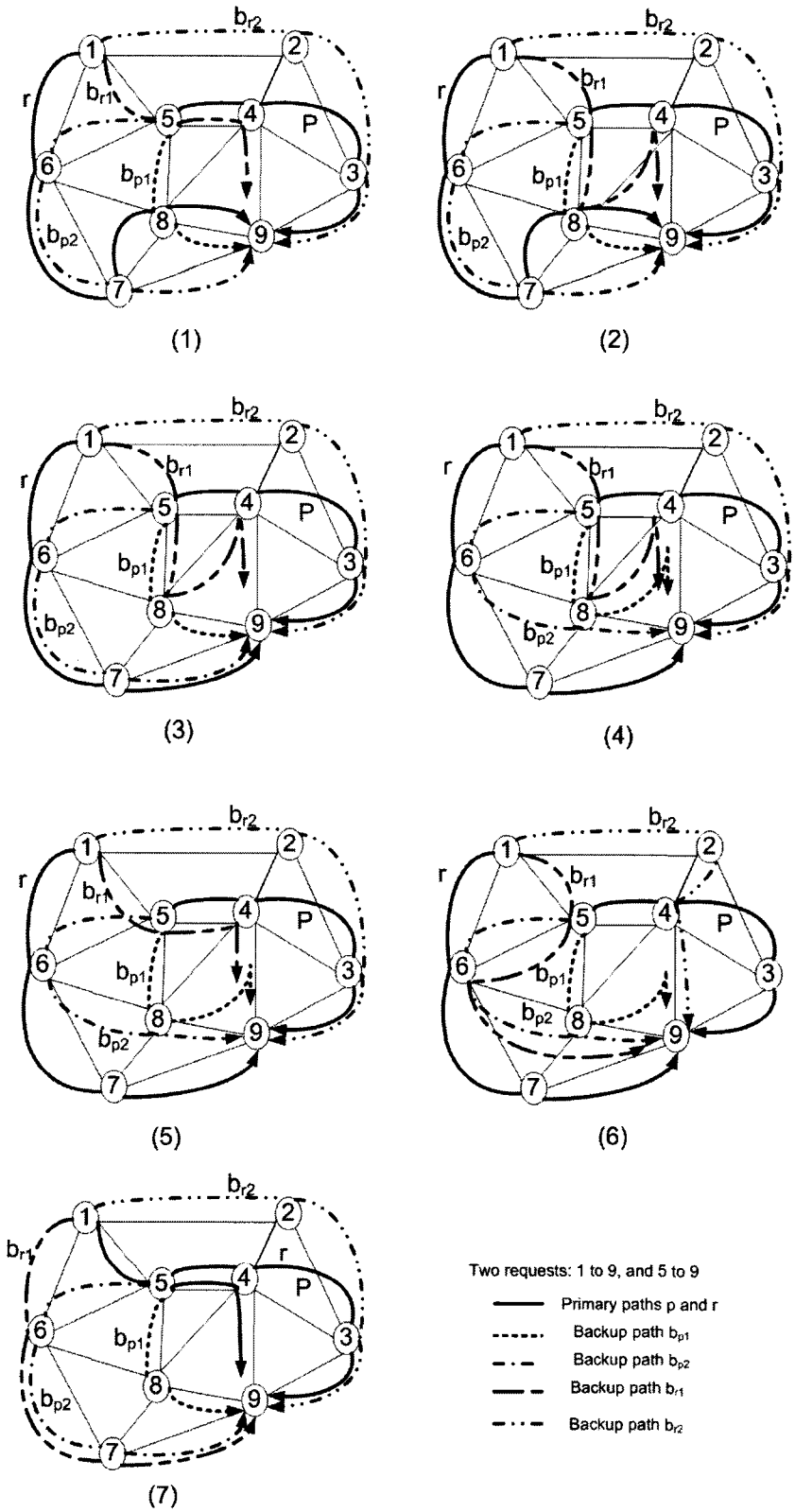

Figure 4.2 Seven primary path-backup path topology relationships.

4.2 Problem Formulation

In this section, we develop the ILP formulation to optimize the capacity utilization for both shared- and dedicated-path protection schemes.

4.2.1 Route Choices for Primary and Backup Paths

For the ILP to optimize the capacity utilization and hence determine the routing and wavelength assignment, a set of alternate routes for each node pair need to be provided as given information to the ILP. In practice, the number of routes has to be restricted. "Eligible routes" [39] can be determined by using hop-limit and distance-limit. The number of equations for the ILP grows rapidly as the number of eligible routes increases, especially in the case of existence of wavelength continuity constraint. In this work, three successive shortest link-disjoint routes for each node pair are pre-computed and this information is provided to ILP.

4.2.2 Problem Formulations

We assume the following information is given: (a) the network topology represented as a directed graph G, (b) a demand matrix, and (c) alternate routing tables at each node. We assume that three alternate routes, which are link-disjoint, for each node pair, are pre-computed by shortest path algorithm. Each route between s-d pair is viewed as W (number of wavelengths available on the link) wavelength continuous paths, and therefore, we do not have an explicit constraint for wavelength continuity. Our objective is to minimize the total number of wavelengths used on all the links in the network (for both the primary and backup paths), measured by number of wavelength-links. 1 wavelength-link is a wavelength used on a link. The notations used in ILPs are defined as in Section 2.2.2, except that here $K = 3$, as there are three alternate routes for each node pair.

4.2.2.1 ILP1: Dedicated-Path Protection

Objective: The objective is to minimize the total number of wavelengths used on all the links in the network (for both the primary and backup paths).

$$Min \sum_{l=1}^{L} (w_l + s_l) \tag{4.2}$$

1. Link capacity constraint:

$$w_l + s_l \leq W \qquad 1 \leq l \leq L \tag{4.3}$$

2. Demand constraint for each node pair:

$$\sum_{p=1}^{KW} \delta^{i,p} = d_i \qquad 1 \leq i \leq N(N-1) \tag{4.4}$$

3. Primary link capacity constraint: Define the number of primary lightpaths traversing each link.

$$w_l = \sum_{i=1}^{N(N-1)} \sum_{p=1}^{KW} \delta^{i,p} \epsilon_l^{i,p} \qquad 1 \leq l \leq L \tag{4.5}$$

4. Spare capacity constraint: Definition of spare capacity required on link l.

$$s_l = \sum_{i=1}^{N(N-1)} \sum_{r=1}^{KW} \nu^{i,r} \epsilon_l^{i,r} \qquad 1 \leq l \leq L \tag{4.6}$$

5. Primary path wavelength usage constraint:

$$\sum_{i=1}^{N(N-1)} \sum_{p=1}^{KW} \delta^{i,p} \epsilon_l^{i,p} \psi_\lambda^{i,p} + \sum_{j=1}^{N(N-1)} \sum_{r=1}^{KW} \nu^{j,r} \epsilon_l^{j,r} \psi_\lambda^{j,r} \leq 1 \qquad 1 \leq l \leq L, 1 \leq \lambda \leq W \tag{4.7}$$

6. Demand constraint for node pair i: There are two restoration routes for each primary call. Let $x, y, z \in \{0, 1, 2\}$ and $x \neq y \neq z$; $t, u, v \in \{\text{x,y,z}\}$, $t \neq u \neq v$:

$$\sum_{p=tW+1}^{(t+1)W} \delta^{i,p} + \sum_{p=uW+1}^{(u+1)W} \delta^{i,p} = \sum_{r=vW+1}^{(v+1)W} \nu^{i,r} \qquad 1 \leq i \leq N(N-1) \tag{4.8}$$

4.2.2.2 ILP2: Shared-Path Protection

The objective function, link capacity constraint, demand constraint for each node pair, and primary link capacity constraint are same as in dedicated path protection case.

4. Spare capacity constraint: Definition of spare capacity required on link l.

$$s_l = \sum_{\lambda=1}^{W} g_{l,\lambda} \quad 1 \le l \le L \tag{4.9}$$

5. Primary path wavelength usage constraint: Only one primary path can use a wavelength λ on link l, no restoration path can use the same λ on link l:

$$\sum_{i=1}^{N(N-1)} \sum_{p=1}^{KW} \delta^{i,p} \epsilon_l^{i,p} \psi_\lambda^{i,p} + g_{l,\lambda} \le 1 \tag{4.10}$$
$$1 \le l \le L, 1 \le \lambda \le W$$

6. Restoration path wavelength usage constraint:

$$g_{l,\lambda} \le \sum_{i=1}^{N(N-1)} \sum_{r=1}^{KW} \nu^{i,r} \epsilon_l^{i,r} \psi_\lambda^{i,r} \tag{4.11}$$
$$1 \le l \le L, 1 \le \lambda \le W$$

$$N(N-1)KW g_{l,\lambda} \ge \sum_{i=1}^{N(N-1)} \sum_{r=1}^{KW} \nu^{i,r} \epsilon_l^{i,r} \psi_\lambda^{i,r} \tag{4.12}$$
$$1 \le l \le L, 1 \le \lambda \le W$$

For the following constraints, let $m, n \in \{0, 1, 2\}$; $s, s' \in \{(m+1) \bmod 3, (m+2) \bmod 3\}, s \ne s'$; $t, t' \in \{(n+1) \bmod 3, (n+2) \bmod 3\}, t \ne t'$. The primary path of a node pair can be any one of the three alternate paths for this node pair. We use m^{th} path of node pair i as primary path for node pair i, and n^{th} path of node pair j as primary path of node pair j. Once the primary path is chosen, the other two alternate paths are to be used as backup paths. We use s^{th} and s'^{th} path of node pair i as backup paths of node pair i. Similarly, we use t^{th} and t'^{th} path of node pair j as backup paths of node pair j. Let

$$X_\lambda^{i,m} = \nu^{i,mW+\lambda} \psi_\lambda^{i,mW+\lambda} \tag{4.13}$$

7. Constraints for backup multiplexing rules 1, 2, and 3 in Table 4.1:

If $I_{(i,s)(j,n)} = 1, I_{(i,m)(j,t)} = 1$, and $I_{(i,s')(j,t')} = 1$

$$X_{\lambda}^{i,s'} + X_{\lambda}^{j,t'} \leq 1 \tag{4.14}$$
$$1 \leq i < j \leq N(N-1), 1 \leq \lambda \leq W$$

8. Constraints for backup multiplexing rules 4 and 5 in Table 4.1:

Let $\Pi_{(i,s\_min)(j,t)} = MIN(\Pi_{(i,s)(j,t')}, \Pi_{(i,s')(j,t')})$. The value of $\Pi_{(i,s\_min)(j,t)}$ is precomputed to reduce the complexity of equation. We precompute and identify s_min, which is one of two paths s and s', and has minimum number of shared link(s) with path (j,t'). To maximize the sharing of backup capacity, we choose s_min^{th} path of node pair i to be the backup path that should not share backup capacity with backup path of (j,t') in the equation 4.15, as required by backup multiplexing rules 4 and 5 in Table 4.1. Same technique is used in Equation 4.16.

If $I_{(i,s)(j,n)} = 0$, $I_{(i,s')(j,n)} = 0$, $I_{(i,m)(j,t)} = 1$, $I_{(i,s)(j,t')} = 1$, and $I_{(i,s')(j,t')} = 1$.

$$X_{\lambda}^{i,s\_min} + X_{\lambda}^{j,t'} \leq 1 \tag{4.15}$$
$$1 \leq i, j \leq N(N-1), 1 \leq \lambda \leq W$$

9. Constraint for backup multiplexing rule 6 in Table 4.1:

Let $\Pi_{(i,s\_min)(j,t-min)} = MIN(\Pi_{(i,s)(j,t)}, \Pi_{(i,s)(j,t')}, \Pi_{(i,s')(j,t)}, \Pi_{(i,s')(j,t')})$

If $I_{(i,s)(j,n)} = 0$, $I_{(i,s')(j,n)} = 0$, $I_{(i,m)(j,t)} = 0$,$I_{(i,m)(j,t')} = 0$, $I_{(i,s)(j,t')} = 1$, $I_{(i,s)(j,t)} = 1$, and $I_{(i,s)(j,t')} = 1$, $I_{(i,s')(j,t)} = 1$, $I_{(i,s')(j,t')} = 1$.

$$X_{\lambda}^{i,s\_min} + X_{\lambda}^{j,t-min} \leq 1 \tag{4.16}$$
$$1 \leq i < j \leq N(N-1), 1 \leq \lambda \leq W$$

For the following constraint, let $m, n \in \{0,1,2\}$; $s, s' \in \{m+1, m+2\}, s \neq s'$; $t, t' \in \{n+1, n+2\}, t \neq t'$.

10. Constraint for rule 7 in Table 4.1:

if $I_{(i,m)(j,n)} = 1, I_{(i,s)(j,t)} = 1$, and $I_{(i,s')(j,t')} = 1$

$$X_{\lambda}^{i,s'} + X_{\lambda}^{j,t'} \leq 1 \tag{4.17}$$
$$1 \leq i, j \leq N(N-1), 1 \leq \lambda \leq W$$

4.3 Results and Discussion

We use CPLEX Linear Optimizer to solve the ILPs. We first demonstrate the working of the ILPs through an example, then present the numerical results for randomly generated demand matrices on a 11-node network modified from NJ LATA network, as shown in Figure 4.3.

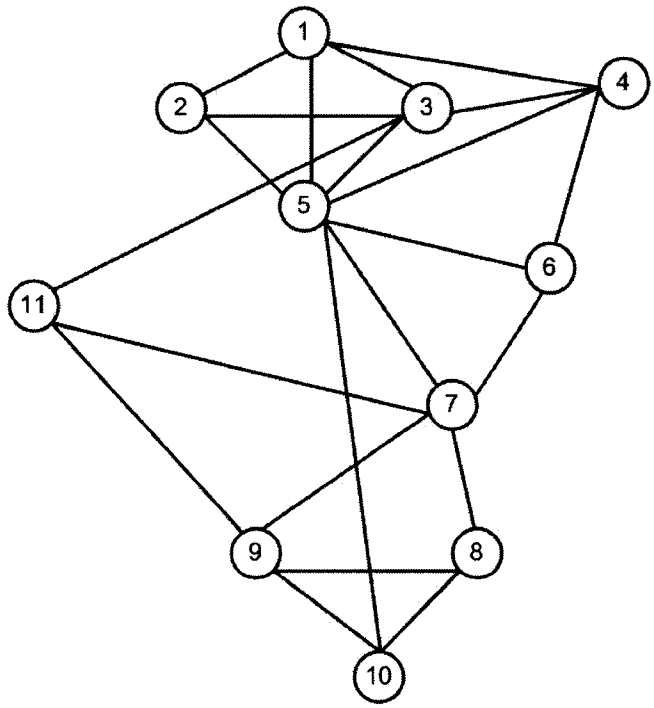

Figure 4.3 Modified NJ LATA network.

4.3.1 An Example Solution

We present an illustration to understand the working of the ILP and to demonstrate the capacity savings obtained by shared-path protection for double-link failures. Consider the 5-node network in Figure 4.1 again. Assume that there is one fiber per link and three wavelengths per fiber.

Let all node pair (i, j) be numbered sequentially in the order of i and j, i.e. node pair

(1, 2) is numbered 1, node pair (1, 3) is numbered 2, and so on. The last node pair (5, 4) is numbered 20. Assume that each of four node pairs 1, 5, 13, 20 have one lightpath request between them. The routes and wavelengths of primary and backup lightpaths for the dedicated-path protection (as solved by ILP1), and the shared-path protection (as solved by ILP2) are illustrated in Table 4.2 and Table 4.3.

Table 4.2 The routes and wavelengths of primary and backup paths under dedicated-path protection

Node pair	Primary lightpath	Backup 1	Backup 2
1	(1,2)—λ_3	(1,3,2)—λ_2	(1,5,4,2)—λ_2
5	(2,1)—λ_3	(2,3,1)—λ_1	(2,4,5,1)—λ_3
13	(4,2,1)— λ_1	(4,3,1)—λ_2	(4,5,1)—λ_2
20	(5,4)—λ_3	(5,3,4)—λ_3	(5,1,2,4)—λ_1

Table 4.3 The routes and wavelengths of primary and backup paths under shared-path protection

Node pair	Primary lightpath	Backup 1	Backup 2
1	(1,3,2)—λ_3	(**1,2**)—λ_3	(1,**5,4,2**)—λ_1
5	(2,3,1)—λ_3	(2,1)—λ_3	(**2,4,5,1**)—λ_3
13	(4,5,1)— λ_2	(**4,2**,1)—λ_1	(4,3,1)—λ_1
20	(5,3,4)—λ_3	(**5,4**)—λ_1	(**5,1,2,4**)—λ_3

In Table 4.2, each reserved wavelength on a backup path is dedicated to a primary path. In contrast, in Table 4.3, λ_3 on links $(5,1)$ and $(2,4)$ is shared by backup paths $2 \rightarrow 4 \rightarrow 5 \rightarrow 1$ and $5 \rightarrow 1 \rightarrow 2 \rightarrow 4$. λ_1 on links $(5,4)$ is shared by backup paths $1 \rightarrow 5 \rightarrow 4 \rightarrow 2$ and $5 \rightarrow 4$. λ_1 on links $(4,2)$ is shared by backup paths $4 \rightarrow 2 \rightarrow$ 1and $1 \rightarrow 5 \rightarrow 4 \rightarrow 2$. λ_3 on link $(1,2)$ is shared by backup paths $1 \rightarrow 2$ and $5 \rightarrow 1 \rightarrow 2 \rightarrow 4$. Note that backup paths $2 \rightarrow 1$ and $4 \rightarrow 2 \rightarrow 1$ can not share backup capacity on their common link $(2,1)$ because of backup multiplexing constraint 3 in Table 4.1. The routings for the primary paths under dedicated- and shared-path schemes are different, because the routing under the shared-path scheme yields maximum saving for total capacity. The shared-path protection scheme uses

a total of 19 wavelength-links, while the dedicated-path protection scheme uses a total of 24 wavelength-links for this demand. The shared-path protection saves about 21% capacity. In link-based protection, dedicated-link scheme uses 28 wavelength-links, and shared links uses 23 wavelength - links [41].

4.3.2 Results on Modified NJ LATA Network

We demonstrate our solution on a modified NJ LATA network shown in Figure 4.3. The modifications include adding links $1 \rightarrow 4$ and $4 \rightarrow 6$, so that the network becomes three connected. We assume the network has one fiber per link for all of the following optimizations.

We demonstrate our solutions on three groups of demand sets, which were generated randomly. Each group consists 10 sets of demand matrix. We wrote a program to generate each set of demand matrix by following steps. Let TNR denotes the desired total number of requests, MNR denotes the maximum number of requests for any node pair.

1. counter = 0;
2. randomly generate source and destination nodes, and the number of requests for this node pair d_i, which is between 1 and MNR;
3. counter = counter + d_i ;
4. if counter $< TNR$, go to step 2;

The TNR for group I, II and III are 40, 60, 100, respectively. The MNR is 4 for group I, II and III. Assume the number of wavelengths per fiber is always sufficient to obtain the feasible solution for each scheme. The optimization results for group I, II and III are shown in Table 4.4, 4.5 and 4.6, respectively. To study the effect of distribution of connection requests, we generated group IV by setting TNR and MNR to be 60 and 8, respectively. The optimization results for group IV are shown in Table 4.7. In all tables, we denote wavelength-links by WLS, dedicated-path protection scheme by DPS, and shared-path protection scheme by SPS.

Table 4.4 shows that for a total of about 40 requests the shared-path scheme requires between 22.3 - 33.4% smaller total capacity than dedicated-path scheme. For a total of about

Table 4.4 The optimization results for request group I

Request set	Number of node pairs	Total requests	WLS used by SPS	WLS used by DPS	Saving	Primary by SPS	Primary by DPS
1	16	41	213	288	26.0	82	59
2	22	41	218	310	29.7	78	68
3	14	40	237	307	22.8	80	75
4	17	40	240	322	25.5	83	77
5	19	40	220	314	24.3	82	65
6	17	42	224	314	23.3	84	73
7	12	41	234	320	26.9	79	67
8	16	41	282	363	22.3	103	86
9	22	40	227	341	33.4	90	83
10	17	41	241	321	24.9	94	80
				average	27.0		

60 connection requests, Table 4.5 shows that the shared-path scheme saves between 26.7 - 34.3% of the total capacity. For a total of about 100 requests, shared-path scheme saves between 27.0 - 37.5% of the total capacity, as shown in Table 4.6. We calculated the capacity used by primary paths for group I, shown in columns 7 and 8 of Table 4.4. Results show that the average primary capacity for shared-path scheme is 14% higher than the average primary capacity for the dedicated-path scheme.This is due to the factor that in order to yield more saving by sharing backup capacity, sometimes the shared-path scheme uses a longer primary path than the dedicated-path scheme.

Among groups I to III, The group III obtains the most average saving and group I gets the least average saving in the total capacity. This is due to the fact that the number of node pairs in the demand matrix increases from group I to III as TNR increases from group I to III. This leads to more sharing in backup capacity. The group II gets more average saving than group IV, which has same number of TNR, but smaller number of node pairs compared to group II. This suggests that the demand matrix with connection requests distributed more evenly (as in the case in group III) will have more chances to share backup capacity, thus saves more in total capacity.

Table 4.5 The optimization results for request group II

Request set	Number of node pairs	Total requests	WLS used by SPS	WLS used by DPS	Saving
1	26	61	285	429	33.5
2	25	62	318	461	31
3	28	63	363	533	31.9
4	26	60	308	469	34.3
5	21	60	356	486	26.7
6	29	61	379	526	27.9
7	26	60	319	460	30.6
8	24	61	347	480	27.7
9	25	61	338	480	29.6
10	21	62	382	521	26.7
				average	29.93

4.3.3 Comparison with Link-based Methods

To compare the path-based protection methods with link-based methods, we conducted optimization for group I, with both dedicated- and shared-link methods presented in [?]. The results are summarized in Table 4.8 (Shared-link scheme is denoted as SLS, and dedicated-link scheme is denoted as DLS in the tables). Comparison between the results in Table 4.4 and Table 4.8 shows that for the given network, the path-based methods are more efficient in the total capacity utilization than the link-based methods, and on average, the dedicated-path scheme yields better performance than share-link scheme. There are no feasible solutions for some of the demand matrices in dedicated-link scheme. It is due to the fact that in the link-based methods, the backup paths have to use the same wavelength as the primary paths and in the dedicated-link scheme, it is easy for conflicts to occur between the two backup paths for the two links on the same primary path [41].

Table 4.6 The optimization results for request group III

Request set	Number of node pairs	Total requests	WLS used by SPS	WLS used by DPS	Saving
1	43	100	456	729	37.5
2	44	101	521	803	35.1
3	37	100	541	818	33.9
4	48	101	546	798	31.6
5	41	101	555	805	31.0
6	38	102	559	818	31.7
7	36	102	571	823	30.6
8	48	103	562	827	32.0
9	36	101	492	739	33.4
10	38	101	607	833	27.0
				average	32.3

4.4 Summary

We presented a path-based double-link failure recovery model, in which two backup paths are provided for each node pair and resources are reserved for each connection. We developed the rules for identifying the scenarios when backup paths can share their backup capacity without violating 100% restoration guarantee. The shared-path scheme provides significant total capacity saving (up to 37.5%). We also found that the backup multiplexing provides more saving for the demand sets that distribute the connection requests more evenly. For the double-link failure recovery methods, path-based methods are more efficient in total capacity utilization than link-based methods. Dedicated-path scheme performs better than shared-link scheme in total capacity utilization on average.

Table 4.7 The optimization results for request group IV

Request set	Number of node pairs	Total requests	WLS used by SPS	WLS used by DPS	Saving
1	14	65	342	436	21.55
2	15	65	359	499	28.0
3	13	62	385	489	21.3
4	14	62	383	470	18.5
5	16	60	380	507	25.0
6	13	60	378	501	24.5
7	12	64	355	449	20.9
8	16	67	402	548	26.6
9	14	63	415	493	15.8
10	14	60	402	544	26.1
				average	23.0

Table 4.8 The optimization results for request group I using link-based

Request set	Number of node pairs	Total requests	WLS used by SLS	WLS used by DLS	Saving
1	16	41	301	349	13.8
2	22	41	344	infeasible	NA
3	14	40	364	infeasible	NA
4	17	40	371	infeasible	NA
5	19	40	328	infeasible	NA
6	17	42	360	infeasible	NA
7	12	41	320	393	18.6
8	16	41	416	infeasible	NA
9	22	40	439	infeasible	NA
10	17	41	397	452	12.2

CHAPTER 5. Survivable Design in Light Trail Networks

5.1 Introduction

The explosive growth in IP traffic in the last decade has triggered a lot of research activities in devising new high-speed transmission and switching technologies. Wavelength division multiplexing (WDM) has emerged as a dominating transmission technology for the next generation IP backbone network with the capability of supporting a number of gigabit wavelength channels in a single fiber. In a typical WDM optical network, the connection between end users are supported by establishing an all-optical channel, namely lightpath, from the source to the destination. Signals are delivered transparently between end terminals without being terminated in the core network. This bit-rate and protocol transparency is a key feature for any backbone network.

One challenging problem for this wavelength switched optical network is the huge opto-electronic bandwidth mismatch. Once a lightpath is established, the entire wavelength is used exclusively by its source and destination node-pair (s-d pair), and no wavelength multiplexing between multiple nodes along the lightpath is allowed. Therefore, the wavelength capacity could be severely underutilized for IP bursts unless the wavelength is filled up by the efficiently aggregated IP traffic. A recently proposed concept named *light trail* [44] offers a strong candidate for supporting IP traffic over optical networks. Light trail architecture can be implemented using mature components that allows fast provisioning of network resource. Hence, in comparison to optical packet switching (OPS) [45, 46, 47], light trail requires neither the high speed electrical header processing for each packet, nor big optical buffering at a node. Moreover, the exclusion of fast switching at packet/burst level, combined with the flexible provisioning for diverse traffic granularity make the light trails superior to conventional circuit

and burst switched architecture.

Due to the huge bandwidth involved in WDM optical transporting networks, any link failure that leaves fiber unusable will have catastrophic results. Survivability is more predominant in light trail networks because one single link failure could cause failures of a set of light trails, each of which carries multiple connections. In this chapter, we study survivable light trail design. The rest of chapter is organized as follows. Section 5.2 is a brief introduction to light trail concept. Two protection schemes that can provide 100% protection in optical layer are proposed and compared in Section 5.3. A formal statement of light trail design problem is given in Section 5.4 followed by an integer linear programming (ILP) formulation for solving this optimization problem. Section 5.5 presents numerical results obtained from our experiments. Section 5.6 concludes this chapter.

5.2 Light Trail Introduction

A light trail is a unidirectional *optical trail* between the start node and the end node. It is similar to a *lightpath* with one important difference that the intermediate nodes can also access this unidirectional trail. In light trails, the wavelength is shared in time and the medium access is arbitrated by control protocol among the nodes that try to transmit data simultaneously, that is, upstream nodes have higher priorities than lower stream nodes. The readers are referred to [44] for the details of light trails architectures. Here we provide a brief introduction to light trails.

5.2.1 Illustration Example

Consider a 4-node light trail shown in Figure 5.1, which starts from node 1, passes through node 2, node 3 and ends at node 4. Each of the nodes 1, 2 and 3 are allowed to send data to any of their respective downstream nodes without the need for optical switch reconfiguration. Every node receives the data from the upstream nodes, but only the corresponding destination node(s) will accept the data packets while other nodes will ignore them. An out-of-band control signal carrying information pertaining to the set up, tear down and dimensioning of light trails

is dropped and processed at each node in the light trail. Since a light trail is unidirectional, a light trail with N_T nodes offers up to $\begin{pmatrix} N_T \\ 2 \end{pmatrix}$ optical connections along the trail. This

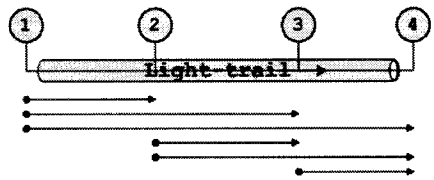

Figure 5.1 Illustrative example of traffic streams in a light trail.

example shows that light trails offer a method to group a set of nodes at the physical layer. Therefore, in contrast to optical burst switching (OBS) [48, 49, 50, 51], there is no need to configure switches for each IP burst when using light trails to transport IP traffic. In fact, this leads to an excellent provisioning time and an order of magnitude better utilization than OBS under the similar situation [44].

5.2.2 How Does It Work?

Figure 5.2 provides a typical node structure in light trail framework. In Figure 5.2, the multiple wavelengths from the input link are de-multiplexed and then sent to corresponding light trail switches. A portion of the signal power goes to the local receiver, the remaining signal power passes through an optical shutter which is typically an AOTF (Acousto-Optic Tunable Filter). Figure 5.3 depicts a connection of four light trail nodes and the corresponding ON/OFF switch configurations. The direction of communication is from node 1 to node 4. The optical shutter is set to *OFF* state at the start and end nodes of the light trail, such that the signal is blocked from travelling further. For an intermediate node along the light trail, the optical shutter is set to *ON* state to allow the signal to pass through the node. We thereby obtain a unidirectional light trail from the start node to the end node. No switch reconfiguration is required after the initial light trail setup. Due to the power loss within the light trail, which mainly comes from the power splitting at each node, the length of a light trail is limited and can be estimated in terms of hop-length. The expected length of a light

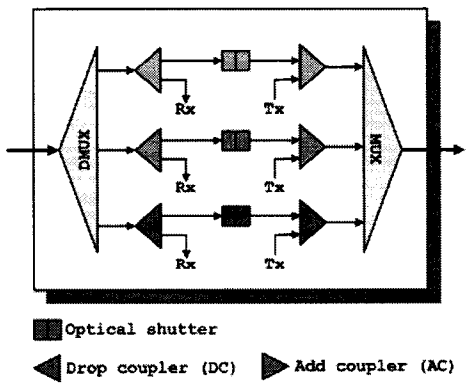

Figure 5.2 An example node structure in light trail framework.

trail is 5 hops [44].

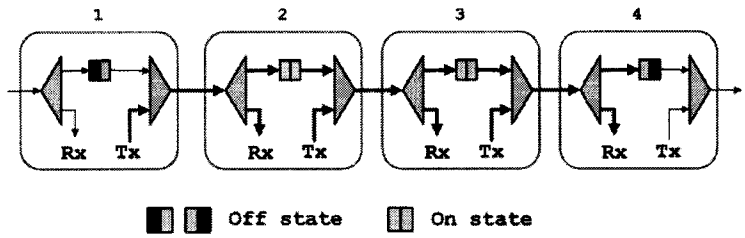

Figure 5.3 An example connection of four light trail nodes.

5.2.3 Why Light Trails?

Current technologies that transport IP centric traffic in optical networks are often too expensive, due to their reliance on expensive optical and opto-electronic approach. Consumers generate diverse granularity traffic and service providers need technologies that are affordable and seamlessly upgradable. The light trail offers a technologically exclusive solution that enables a number of salient features and is practical. It exhibits a set of properties that distinguishes and differentiates from other platforms. The following three characteristic properties of light trails make possible this differentiation:

- Light trails are built using mature components that are configured in such a way that

allows extremely fast provisioning of network resources. This allows for dynamic control for the fluctuating bandwidth requirements.

- Light trails offer a method to group a set of nodes at the physical layer to create optical multicasting - a key feature for the success of many applications.

- The maturity of components leads to the implementation of light trails in a cost effective manner resulting in economically viable solutions for mass deployment.

5.3 Restoration Models in Light Trail Architecture

Survivability is a critical issue in the design of light trail of a failure optical network as due to the fact that a single link failure disrupts all the light trails that use the link. Each light trail carries multiple connections. Therefore the effects would be catastrophic. For instance, if a failed link has W wavelength, it can carry up to W light trails. Each light trail contains up to $\frac{n_w(n_w-1)}{2}$ s-d pairs, where n_w denotes the number of nodes in the wth light trail, $w = 1, 2, \ldots, W$. Therefore, in the worst case a link failure may disrupt up to $\sum_{w=1}^{W} \frac{n_w(n_w-1)}{2}$ connections. To provide 100% protection in WDM layer of light trail architecture implies that backups need to be provided at the time of establishing connections.

Recall that a key difference between the light trail and lightpath architectures is that the intermediate nodes in a light trail can also have access to the medium. Thus the restoration model for a light trail architecture is different from that in lightpath architecture as all node pairs on light trail need to be protected and assigning an alternate path may not be possible. We discuss two possible protection schemes here, namely *connection based protection* and *link based protection.* In the following it is assumed that there is no more than one link failure at any time.

5.3.1 Connection Based Protection

For each connection request d_{st}, the resources are allocated to a primary connection in a light trail LT_1 and a backup connection in another light trail LT_2. LT_1 and LT_2 are link-

disjoint. The primary connection is a working connection when there is no link failure. If a link on LT_1 fails, the failure information is propagated through the control channel. The source node s of the request receives the failure information, it starts to transmit the data on LT_2 to the destination t through the backup connection.

The scheme is explained through an example, shown in Figure 5.4. Suppose there are two light trails, LT_1: $1 \rightarrow 2 \rightarrow 3 \rightarrow 4$, and LT_2: $2 \rightarrow 6 \rightarrow 5 \rightarrow 4$. LT_1 and LT_2 are link-disjoint. There is a connection request from node 2 to node 4. In this case, a primary connection between node 2 and 4 is established on light trail LT_1 with the backup connection on light trail LT_2. Suppose link $2 \rightarrow 3$ on LT_1 fails, then light trail LT_1 cannot be used. When this failure information reaches source node 2, the source node 2 starts to transmit data using backup connection on LT_2.

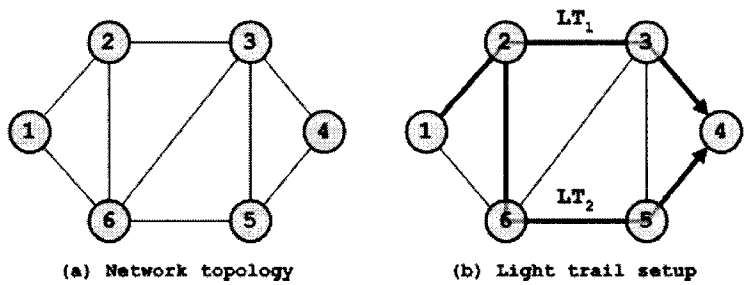

Figure 5.4 An example for connection based scheme.

5.3.2 Link Based Protection

In this case, for each link on a light trail, a backup sub-light trail is provided. When a link on a light trail fails, a light trail is rerouted around the failed link and use the backup sub-light trail.

Consider the same example again. Suppose for each of link on LT_1, there is a backup sub-light trail. The backup sub-light trail for link $3 \rightarrow 4$ is $3 \rightarrow 5 \rightarrow 4$ as shown in Figure 5.5. If link $3 \rightarrow 4$ fails, the information about the failure and the sub-light trail of link $3 \rightarrow 4$ is sent along the control channel (it is assumed that there exists bidirectional control channel). When

the message reaches source Node 1, Node 1 will send a fault management message, which is similar to light trail set up message, along the control channel to intermediate nodes (Node 2, 3, and 5) and end node 4. These nodes then configure the optical shutter and form a new light trail $1 \rightarrow 2 \rightarrow 3 \rightarrow 5 \rightarrow 4$.

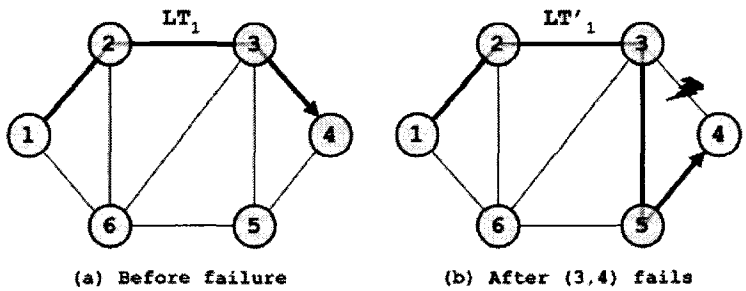

Figure 5.5 An example for link based protection scheme.

5.3.3 Comparison of Connection Based and Link Based Protections

The connection based protection has following advantages over link based protection.

- Restoration time: In the connection based protection, as soon as the failure information message reaches the source node of a connection that is using the light trail, the source node can immediately start using the backup connection on another light trail to continue the transmission. The maximum restoration time is transmission time of the control message. Link-based approach requires the ability to identify a failed link at both ends, which makes restoration more difficult when a node failure happens. In link based protection, after the failure information reaches the source node of the failed light trail, the source node will have to initiate a light trail setup process, i.e. setting up a light trail that includes the remaining part of the original light trail and the nodes on the backup sub-light trail of failed link. This takes much more time than the restoration in connection based protection.

- The length of the light trail: As shown in the example, the restored light trail in a link based protection scheme is longer than the original light trail. As discussed previously, the length of the light trail is an important parameter that is related to bit-error-rate. This again limits the choice for link-based protection. Thus, link-based restoration is likely to perform poorly in this regard.

From the above discussion, it is concluded that the connection based protection is likely to be more practical for light trail architecture. Therefore only connection based protection is considered in the rest of the paper.

5.4 Survivable Light Trail Design

The major issue in the design of survivable light trail network is to identify a set of light trails to carry the given traffic and provide 100% protection against single link failure. The survivable light trail network design problem is defined as follows.

Given a graph $G(V, E)$, where $|V| = N$, and traffic matrix $D_{N\times N}$, identify a minimum number of light trails to carry the given traffic in such a way that for each connection request, there is a primary connection established in one light trail and resources are reserved in another light trail for backup connection. Two light trails for each s-d pair are link-disjoint.

Recall that the maximum hop-length of a light trail is denoted by Tl_{max}. We use a two-step approach similar to the one described in [52]. In the first step, a traffic matrix preprocessing is conducted to recursively divide a long hop into multiple hops. For a request between the source node s and the destination node t, it is required that there are at least two link disjoint light trails that both pass through node s and node t, and satisfy the light trail length limit. We modify the traffic matrix preprocessing algorithm in [52]. First we find the distance matrix $H_{N\times N} = \{h_{st}\}$ and secondary distance matrix $H'_{N\times N} = \{h'_{st}\}$, where h_{st} denotes the hop length of shortest path from node s to node t, and h'_{st} denotes the second shortest path from node s to node t. The second shortest path from node s to node t is found by applying Dijkstra's algorithm in the graph in which all the links on the first shortest path from node s to node t are removed. For a connection request between node s and t, if either $h_{st} > Tl_{max}$ or

$h'_{st} > Tl_{max}$, it is not possible to accommodate both the primary and backup connections of this request on two direct and link disjoint light trails. Thus this request needs to go through multiple hops. The modified traffic matrix preprocessing algorithm recursively divides each request that has $h_{st} > Tl_{max}$ or $h'_{st} > Tl_{max}$ into multiple hops, and returns a modified traffic matrix. In the modified traffic matrix, each non-zero element has at least two link disjoint paths for which $h_{st} > Tl_{max}$ and $h'_{st} > Tl_{max}$. The pseudocode for modified preprocessing algorithm is shown in Figure 5.6.

input Graph $G = (V, E)$ and a traffic matrix $D_{N\times N}$.
output Rearranged traffic matrix $D_{N\times N}$ and the distance matrix $H_{N\times N}$ and the secondary distance matrix $H'_{N\times N}$.
algorithm Modified traffic matrix preprocessing
begin
Apply *Dijkstra's shortest path algorithm* to calculate the distance matrix $H_{N\times N}$, and the secondary distance matrix $H'_{N\times N}$.
while (found (s,t) : $d_{st} > 0$, $h_{st} > Tl_{max}$ or $h'_{st} > Tl_{max}$)
{

1. Pick an intermediate node n:
   $n = arg\ min_{v\in V}\{d_{vt} | h_{sv} \leq Tl_{max}$ and $h'_{sv} \leq Tl_{max}\}$;
2. Update traffic matrix $D_{N\times N}$:
   (a) $d_{sn} \leftarrow d_{sn} + d_{st}$;
   (b) $d_{nt} \leftarrow d_{nt} + d_{st}$;
   (c) $d_{st} \leftarrow 0$.

}
end

Figure 5.6 Modified traffic matrix preprocessing for restoration in light trail networks

The next step is to develop an ILP formulations to optimize the capacity utilization in terms of number of light trails, with the given network topology and refined traffic matrix obtained from the *traffic matrix preprocessing*. The objective is to find a minimum number of light trails that are required for the system.

5.4.1 ILP Formulation: Connection Based Protection

Given the network topology $G(V, E)$, and the traffic matrix obtained from *traffic matrix preprocessing*, one first lists all possible paths with the hop-length limit constraint for each *s-d* node pair. This can be accomplished by using *breadth first search* for each node. These eligible paths form a set of all possible light trails. Among all the possible choices, an optimal set of paths is chosen to form the light trail network such that the total number of light trails are minimized and the demand constraint and protection constraint are met. This problem is formulated as an ILP optimization problem. It is also assumed that each request cannot be split into multiple parts.

5.4.1.1 Notation

The network topology is represented as a directed graph $G(V, E)$ with $|V| = N$ nodes and $|E| = L$ links with W wavelengths on each link. The following notations are used.

- $n = 1, 2 \ldots, N$: Number assigned to each node in the network.
- $p, p_1, p_2 = 1, 2 \ldots, P$: Number assigned to a path in the network.
- $i, j, k = 1, 2, \ldots, N(N-1)$: Number assigned to a node pair. The source and destination nodes of a connection request forms a node pair.

The following notations are used for path related information.

- δ_p^i: Path indicator. This takes a value of one if primary connection for request i is established on light trail p; zero otherwise (binary variable).
- ν_p^i: Path indicator. This takes a value of one if backup connection for connection request i is established on light trail p; zero otherwise (binary variable).
- ψ_p^i: Node pair indicator. This takes a value of one if node pair i is on path p; zero otherwise (data).

- h_p: Light trail usage indicator. This takes a value of one if path p is used for carrying any connection (primary or backup); zero otherwise (binary variable).
- d_i: Demanded capacity of connection request i (data).
- I_{p_1,p_2}: This takes a value of one if p_1 and p_2 are link-disjoint; zero otherwise (binary data).

5.4.1.2 Objective

Minimize number of light trails. If a path p is used for carrying any connection (primary or backup), it becomes a light trail and h_p is set to one.

$$min \sum_{p=1}^{P} h_p \tag{5.1}$$

5.4.1.3 Constraints

1. *On demand constraint for each node pair:* For each request, there is one primary connection on one light trail, and a backup connection in another light trail.

$$\sum_{p=1}^{P} \delta_p^i \psi_p^i = 1 \qquad 1 \leq i \leq N(N-1) \tag{5.2}$$

$$\sum_{p=1}^{P} \nu_p^i \psi_p^i = 1 \qquad 1 \leq i \leq N(N-1) \tag{5.3}$$

2. *On topology diversity of primary and backup connections:* The primary and backup connections for a request are established on two link-disjoint light trails.

$$(\delta_{p_1}^i \psi_{p_1}^i + \nu_{p_2}^i \psi_{p_2}^i)(1 - I_{p_1,p_2}) \leq 1 \qquad 1 \leq i \leq N(N-1), 1 \leq p_1, p_2 \leq P \tag{5.4}$$

3. *On link capacity constraints:* The total demand of all connections on one light trail cannot exceed one wavelength capacity. The first term represents the capacity used by primary connections on light trail p. The second term represents the capacity used by backup connections on light trail p.

$$\sum_{i=1}^{N(N-1)} \delta_p^i \psi_p^i d_i + \sum_{i=1}^{N(N-1)} \nu_p^i \psi_p^i d_i \leq C \qquad 1 \leq p \leq P \tag{5.5}$$

4. *On light trail identification constraints:* If one or more of the primary or backup connections uses a path, then this path is a light trail.

$$h_p \leq \sum_{i=1}^{N(N-1)} \delta_p^i \psi_p^i + \sum_{i=1}^{N(N-1)} \nu_p^i \psi_p^i \quad 1 \leq p \leq P \tag{5.6}$$

$$2N(N-1)h_p \geq \sum_{i=1}^{N(N-1)} \delta_p^i \psi_p^i + \sum_{i=1}^{N(N-1)} \nu_p^i \psi_p^i \quad 1 \leq p \leq P \tag{5.7}$$

5.5 Numerical Results

The above formulation is solved for some example networks, a 6-node network shown in Figure 5.4 (a) and a 10-node network shown in Figure 5.7.

To simplify the problem, the links are assumed to be bidirectional with the same length. As observed earlier, the number of potential light trails, i.e. possible paths in a network increases rapidly as the number of nodes in the network increases. For example, for the two example networks, the number of possible paths are 120 and 448, respectively. This makes it difficult to solve ILP for large-sized network and for large number of connection requests. In such cases, heuristic strategies have to be adopted to solve the survivable light trail design problem in big network with large number of connection requests.

5.5.1 A Simple Example

A simple example is presented to understand the solution obtained from the ILP formulation, which optimally identify the light trails covering all the working connections and corresponding backup connections. For the network shown in Figure 5.4, a traffic matrix shown in Table 5.1 is to be routed. The integer numbers indicates the request capacity in unit of OC-1 (51.84 Mbps), while the entire wavelength capacity is OC-48. The hop length limit is set to be 3, that is, $Tl_{max} = 3$. Table 5.2 gives the resulting light trails that covers all the connection

requests and their corresponding backup connections. The notation (s, d) and $(s, d)_b$ in column 4 denote primary and backup connections, respectively.

Table 5.1 Requests matrix for a 6-node network.

	1	2	3	4	5	6
1	0	11	6	0	14	8
2	0	0	0	0	5	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	19	0

Table 5.2 Resulting light trails for example request matrix I.

No.	Light Trails	Hops	Accommodated *s-d* pairs	load
1	{1, 2, 3}	2	$(1,2), (1,3)_b$	17
2	{1, 2, 6, 5}	3	$(2,5), (6,5), (1,5)_b, (1,6)_b$	46
3	{1, 6, 2}	2	$(1,6), (1,2)_b$	19
4	{1, 6, 3, 5}	3	$(1,3), (1,5), (6,5)_b$	39
5	{2, 3, 5}	2	$(2,5)_b$	5

In order to provide 100% protection for a single link failure, each request is allocated resource for a working connection in one light trail and reserved resource for its backup connection in another light trail. The two light trails are disjoint. In Table 5.2, working connection for request $(1,2)$ uses light trail $1 \rightarrow 2 \rightarrow 3$, while backup connection for this request is accommodated on light trail $1 \rightarrow 6 \rightarrow 2$. Similarly, for request (1, 3), two link disjoint light trails $1 \rightarrow 6 \rightarrow 3 \rightarrow 5$ and $1 \rightarrow 2 \rightarrow 3$ are used. 5 light trails and a total of 12 wavelength-links are used for this request matrix.

5.5.2 Experiment I

Table 5.3 provides a randomly generated dense traffic matrix for the 6 node network. It is assumed that the hop-length limit $Tl_{max} = 3$. From the topology it is observed that all *s-d* pairs have paths within this hop-length limit, hence, the *traffic matrix preprocessing* is

not needed. Since the experiments are performed on small fractional wavelength requests, the number of wavelengths on each link is not a critical constraint. For this example $W = 4$ is sufficient, although there is no constraint being put on number of wavelengths. Table 5.4 presents the results from solving the ILP formulation with hop-length limit $Tl_{max} = 3$.

Table 5.3 Requests matrix for a 6-node network.

	1	2	3	4	5	6
1	0	7	6	9	19	17
2	27	0	3	6	28	2
3	14	3	0	19	31	9
4	26	5	29	0	5	23
5	27	20	20	17	0	14
6	9	30	1	1	1	0

Table 5.4 shows 21 light trails that are needed to carry the primary and backup connections. The traffic assignment obtained from solving ILP formulation is also listed. For each light trail, the amount of total traffic carried is shown in the right most column in Table 5.4. Notice that most of the light trails are fully or almost fully occupied. Hence, the resource utilization is quite high.

5.5.3 Example II

An experiments is performed on a topology given in Figure 5.7. Table 5.5 is a randomly generated traffic matrix for the 10-node network. The request capacity for each node pair is uniformly distributed between 0 and 11. It is assumed that the hop-length limit $Tl_{max} = 4$. Applying the preprocessing algorithm in Figure 5.6, the second shortest path between node 3 and node 9 has length of 5 hops. Therefore it needs to be divided into multiple hops. The preprocessing algorithm re-arrange the traffic $d_{3,9}$ to $d_{3,7}$ and $d_{7,9}$. Similarly, $d_{4,9}$ is reallocated on $d_{4,7}$ and $d_{7,9}$, $d_{4,10}$ is reallocated on $d_{4,8}$ and $d_{8,10}$, $d_{9,3}$ is reallocated on $d_{9,7}$ and $d_{7,3}$, and $d_{9,4}$ is reallocated on $d_{9,7}$ and $d_{7,4}$.

Table 5.6 shows the resulting modified traffic matrix in which all the requests have at least two paths satisfying the hop length constraint. The ILP solution identifies 48 light trails that

Table 5.4 Resulting light trails.

No.	Light Trails	Hops	Accommodated s-d pairs	Load
1	{1, 2, 3, 4}	3	$(1,2),(1,4),(1,3)_b,(2,4)_b,(3,4)_b$	47
2	{1, 6, 3, 2}	3	$(1,3),(1,2)_b,(6,2)_b$	43
3	{1, 6, 5, 4}	3	$(1,4)_b,(1,5),(1,6),(6,4),(6,5)$	47
4	{2, 3, 6, 1}	3	$(2,1),(2,6),(3,1),(2,3)_b$	46
5	{1, 2, 6, 3}	3	$(2,3),(1,6)_b$	20
6	{2, 6, 5, 4}	3	$(2,4),(2,5)_b,(2,6)_b$	36
7	{1, 2, 3, 5}	3	$(2,5),(1,5)_b$	47
8	{3, 2, 6, 5}	3	$(3,2),(3,5),(3,6)$	43
9	{4, 3, 2, 1}	3	$(3,1)_b,(4,1),(4,2)_b$	45
10	{4, 5, 6, 2}	3	$(4,2),(4,6),(5,2)_b$	48
11	{4, 3, 5, 6}	3	$(4,3),(4,5),(5,6)_b$	48
12	{5, 6, 2, 1}	3	$(5,1),(6,1)$	36
13	{5, 3, 2, 1}	3	$(5,2),(2,1)_b$	47
14	{5, 6, 3, 4}	3	$(5,3),(6,3),(5,4)_b,(6,4)_b$	39
15	{3, 5, 4}	2	$(3,4),(5,4)$	36
16	{4, 5, 3, 6}	3	$(5,6),(4,5)_b,(4,3)_b$	48
17	{4, 3, 6, 2}	3	$(6,2),(3,2)_b$	33
18	{6, 2, 3, 5}	3	$(3,5)_b,(6,3)_b,(6,5)_b$	33
19	{4, 3, 6, 1}	3	$(3,6)_b,(6,1)_b,(4,6)_b$	41
20	{4, 5, 6, 1}	3	$(4,1)_b$	26
21	{5, 3, 6, 1}	3	$(5,3)_b,(5,1)_b$	47

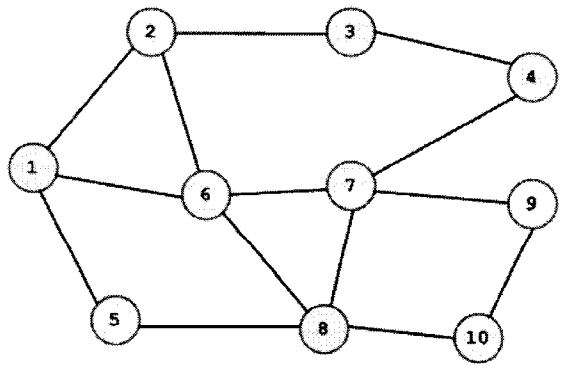

Figure 5.7 A 10-node example network.

Table 5.5 Traffic matrix for a 10-node network

	1	2	3	4	5	6	7	8	9	10
1	0	5	11	10	4	5	4	6	6	10
2	8	0	5	5	1	3	1	11	7	2
3	3	0	0	3	0	2	9	4	10	9
4	8	2	11	0	11	6	11	6	9	4
5	11	7	7	6	0	11	3	2	9	9
6	8	9	7	5	4	0	11	8	10	9
7	9	7	11	9	1	10	0	4	11	2
8	6	0	10	4	2	4	4	0	2	9
9	2	9	10	2	6	9	9	8	0	9
10	11	0	10	0	8	10	8	11	4	0

are needed to carry the traffic. The actual light trails and traffic assignments are omitted due to the space limit. The average amount of traffic carried per light trail is 26.

Table 5.6 Traffic matrix for a 10-node network after preprocessing

	1	2	3	4	5	6	7	8	9	10
1	0	5	11	10	4	5	4	6	6	10
2	8	0	5	5	1	3	1	11	7	2
3	3	0	0	3	0	2	**19**	4	**0**	9
4	8	2	11	0	11	6	**20**	**10**	**0**	**0**
5	11	7	7	6	0	11	3	2	9	9
6	8	9	7	5	4	0	11	8	10	9
7	9	7	**21**	**11**	1	10	0	4	**30**	2
8	6	0	10	4	2	4	4	0	2	**13**
9	2	9	**0**	**0**	6	9	**21**	8	0	9
10	11	0	10	0	8	10	8	11	4	0

5.6 Summary

The concept of light trails has been proposed as a novel architecture designed for carrying finer granularity bursty IP traffic. The exclusion of fast switching at packet/burst level, combined with the flexible dynamic sub-wavelength provisioning make light trail architecture a strong candidate for transporting IP traffic over optical networks.

Due to the nature of light trails, survivability is a more predominant issue in the design of light trail optical networks than it is in traditional wavelength routed optical networks using lightpaths. We propose two protection schemes to provide 100% protection against single link failure, namely *connection based protection* and *link based protection.* Connection based protection scheme has advantages over link based protection scheme, and is more practical for light trail architecture where the hop-length is limited due to power loss. Hence, we adopted connection based protection model and formulated the survivable design problem with the objective to minimize the number of required light trails as an ILP optimization problem. The numerical results obtained from solving our ILP formulation are presented and show that the resulting light trail network achieves good wavelength utilization as well as 100% protection against single link failure.

The ILP formulation produces the optimal solution to the survivable light trail network design problems with static traffic demands. However, the computation time for solving ILP formulation is quite large, and it becomes unmanageable as the size of the network or the number of requests increases. Developing efficient heuristic approaches for solving survivable design problems in light trail networks is one future direction.

CHAPTER 6. Conclusion

Wavelength-division multiplexing (WDM) technology allows building of very large capacity, of the order of terabits per second wide area networks. Such networks provide low error rates and low delay and offer a viable solution to meet the bandwidth demand ever increasing. Survivability is a critical component of WDM network design due to high traffic speed and high vulnerability. In wavelength-routed WDM networks, a new network layer, called the optical layer or WDM layer, is introduced into the layered network architecture. WDM layer protection has been shown to have advantages and has been justified to be necessary. This dissertation has addressed several important survivable design issues in WDM mesh networks.

Capacity efficiency and recovery speed are two important aspects in designing protection mechanisms. Shared backup path protection and p-cycle protection are two most widely studied protection schemes in mesh network protection. Shared path protection has long been believed to be capacity efficient, while p-cycle protection has been reported to have "ring like speed and mesh like efficiency". A recently proposed pre-cross-connected protection concept tries to catch the common ground of above two protection techniques. We conducted comparison study of these protection schemes in terms of both recovery time and capacity efficiency, in the context of WDM wavelength continuous networks. The recovery processes of these schemes are reviewed and recovery times are compared analytically. There are two factors that contribute to fast recovery of p-cycle protection: the time for propagating and processing signaling messages and the time for configuring the cross-connects in the backup route are not needed in p-cycle protection. In contrast, both times are needed in shared path protection. The time to configure the cross-connects in the backup route is the dominant factor. Pre-cross-connected shared path protection eliminates the time to configure the cross-connects in the backup route

by imposing additional constraint in sharing backup capacity. Thereby, pre-cross-connected shared path protection is significantly faster than general shared path protection in recovering from a failure. But it is still slower than p-cycle protection in recovery, because it is path-based protection and the signaling process is still needed.

The problems of optimizing the capacity required for given static traffic are then formulated for these three different schemes. A series of networks that reflect the change of network connectivity are used to study the effect of network connectivity on the capacity performance of these different schemes. The numerical results indicate that general shared path protection and pre-cross-connected shared path protection use less total capacity than p-cycle protection in low-connectivity networks, while they are comparable in high-connectivity networks. Pre-cross-connected shared path protection uses about 10% more capacity than general shared path protection. Pre-cross-connected protection can achieve fast restoration while remaining to be path-based method. Thus, It provides a tradeoff of recovery speed and capacity efficiency, especially in low-connectivity networks.

Dynamic establishment of restorable connections is an important issue. Survivable design for dynamic traffic using p-cycle technique has the potential to achieve both fast recovery and capacity efficiency. We developed a p-cycle based scheme to deal with dynamic traffic in WDM networks. We use a two-step approach. In first step, we find a set p-cycles to cover the network and reserve enough capacity in p-cycles. By doing this, we provision the network built-in resources to be two parts: protection resources and resources available for accommodating the working traffic. The objective of partitioning the resources in this step is to guarantee that the capacity available for routing randomly arriving connection requests will be 100% protected by the reserved protection capacity in the p-cycles. The design also ensures that the p-cycles are preconfigured. In second step, we route the requests as they randomly arrive one by one. We propose two routing algorithms. Compared to the shared path protection, in which a primary path and backup path is determined for each request as it arrives, the p-cycle based protection in this chapter considers the protection in the network as a whole in one step. This leads to less control signaling overhead and less dynamic state information to be maintained. Therefore,

the p-cycle design has the advantage of fast recovery, less control signaling, less dynamic state information to be maintained. To evaluate the blocking performance of proposed method, we compare it with shared backup path protection. Simulation results obtained from ten networks indicate that in high-connectivity or very low connectivity networks, the proposed p-cycle design has similar or even better performance in blocking probability, and thus is a better choice. In medium- or low-connectivity networks, the proposed p-cycle has higher blocking probability than shared path protection. It provides a tradeoff between the recovery speed and the blocking probability.

Although the failure of single component such as a link or a node is the most common failure scenario, it is possible to have multiple links fail simultaneously. We propose a path-based protection method for two-link failures in mesh optical networks. Two link-disjoint backup paths are pre-computed for each source and destination node pair and resources are reserved on the backup paths for each connection request. To reduce reserved backup capacity, backup capacity sharing without compromising the restoration guarantee must be explored. We identify the scenarios where the backup paths can share their wavelengths without violating 100% restoration guarantee (backup multiplexing). We formulate the problem of optimizing the total capacity requirement for both dedicated- and shared-path protection schemes. Numerical results indicate that, backup multiplexing significantly improves the efficiency of total capacity utilization.

The recently proposed *light trail* architecture offers a promising candidate for carrying IP centric traffic over optical networks. The survivable design is a critical part of the integral process of network design and operation. The restoration methods for lightpath protection cannot be applied to light trail architecture because of the important difference that the intermediate nodes on light trail can also access the trail. In chapter 5, We propose and compare two protection schemes, namely *connection based protection* and *link based protection*, that can achieve 100% protection against single link failure. The survivable light trail design problem using connection based protection model is solved using a two-step approach. The numerical results show that the design achieves high wavelength utilization as well as 100% protection

against single link failure. The computation time for solving ILP formulation is quite large, and it becomes unmanageable as the size of the network or the number of requests increases. Developing efficient heuristic approaches for solving survivable design problems in light trail networks is one future direction.

BIBLIOGRAPHY

[1] O. Gerstel and R. Ramaswami, "Optical network survivabilty: A service perspective", *IEEE Communication Magazine*, vol. 38, no. 3, pp. 104–113, March 2000.

[2] I. Chlamtac, A. Ganz, and G. Karmi, "Lightpath communication: An approach to high bandwidth optical WANs," *IEEE Transactions on Communications*, vol. 40, pp1171-1182, July 1992.

[3] D. Zhou and S. Subramaniam, "Survivability in optical networks", *IEEE Network*, vol. 6, no. 14, pp. 16–23, March 2000.

[4] G. Mohan and C. S. R. Murthy, "Lightpath restoration in WDM optical networks", *IEEE Network*, vol. 6, no. 14, pp. 24–32, March 2000.

[5] G. Maier, A. Pattavina, and et al., "Lightpath restoration in WDM optical networks", *Photonic Network Communications*, vol. 4, no. 3/4, pp. 251–269, July 2002.

[6] ITU-T Draft Rec. G.872, "Architecture of optical transport networks", *IEEE Communication Magazine*, SG 13, question 19, Feburary 1999.

[7] T. Y. Chow, F. Chudak and A. M. Ffrench, "Fast optical layer mesh protection using pre-cross-connected trails", *IEEE/ACM Transaction On Networking*, vol. 12, No.3, pp. 539-548, June 2004.

[8] H. Choi, S. Subramaniam, and H.A. Choi, "Loopback recovery from double-link failures in optical networks," *IEEE/ACM Transaction on Networking*, Vol. 12, No. 6, pp. 1119–1130, December 2004.

[9] G. Ellinas, G. Halemariam, and T. Stern, "Protection cycles in mesh WDM networks", *IEEE Journal of Selected Areas in Communication*, vol. 18, no. 10, pp. 1924–37, October 2000.

[10] W. D. Grover and D. Stamatelakis, "Cycle-oriented distributed preconfiguration: Ring like speed and mesh-like capacity for self-planning network Restoration", *Proc. of IEEE ICC*, vol. 1, pp. 737-543, June 1998.

[11] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, part II - restoration", *IEEE ICC*, vol. 3, pp. 2023-2030, June 1999.

[12] L. Sahasrabuddhe, S. Ramamurthy, and B. Mukherjee, "Fault management in IP-over-WDM networks: WDM protection versus IP restoration", *IEEE JSAC*, vol. 20, No. 1, pp. 21-33, January 2002.

[13] B. T. Doshi, S. Dravida, P. Harshavardhana, O. Hauser, and Y. Wang, "Optical Network Design and Restoration", *Bell Labs Technical Journal*, pp. 58-84, January-March 1999.

[14] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, part I: protection," *IEEE INFOCOM*, vol. 2, pp. 744–751, March 1999.

[15] M. Sridharan, M.V. Salapaka, and A.K. Somani, "Operating mesh-survivable WDM transport networks," *SPIE International Symposium on SPIE Terabit Optical Networking: Terabit Optical Networking*, pp. 113–123, November 2000.

[16] M. Sridharan, A.K. Somani, and M.V. Salapaka, "Approaches for capacity and revenue optimization in survivable WDM networks," *Journal of High Speed Networks*, vol. **10**, no. 2, pp. 109 – 125, August 2001.

[17] R. R. Iraschko, M. H. MacGregor and W.D. Grove, " Optimal capacity placement for path restoration in STM and ATM mesh-survivable networks," *IEEE/ACM Transaction on Networking* vol. 6, no. 3, pp. 325-336, June 1998.

[18] G. Mohan and A.K. Somani, "Routing dependable connections with specified failure restoration guarantees in WDM networks," *IEEE INFOCOM*, pp. 1761–1770, March 2000.

[19] G. Mohan, C.S.R. Murthy, and A.K. Somani, "Efficient algorithms for routing dependable connections in WDM optical networks," *IEEE/ACM Transactions on Networking*, vol. 9, no. 5, October 2001, pp. 553-566.

[20] G. Li, D. W, C. Kalmanek, and R. Doverspike, "Efficient distributed restoration path selection for shared mesh restoration," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, October 2003, pp. 761-771.

[21] W. D. Grover and D. Stamatelakis, "Bridging the ring-mesh dichotomy with p-cycles", *Proc. of DRCN workshop*, pp. 92-104, April 2000.

[22] W. D. Grover and J. Doucette, "Advances in optical network design with p-cycles: Joint optimization and pre-selection of candidate p-cycles," *Proceedings of IEEE/LEOS Summer Topicals*, pp. 49-50 (paper WA2), Mont Tremblant, PQ, Canada, July 2002.

[23] C. Liu and L. Ruan, Finding good candidate cycles for efficient p-cycle network design, *Proceedings of the Thirteenth International Conference on Computer Communications and Networks (ICCCN)*, pp. 321-326, October 2004.

[24] H. Zhang and O. Yang, Finding protection cycles in DWDM netowrks, *Proceedings of IEEE ICC*, pp. 2756-2760, April/May 2004.

[25] J. Doucette, D. He, W. D. Grover, and O. Yang, "Algorithmatic approaches for efficient enumeration of candidate p-cycles and capacitated p-cycle network design," *Proceeding of DRCN 2003*, pp. 212-220, October 2003.

[26] D. A. Schupke, C. G. Gruber, and A. Autenrieth, "Optimal configuration of p-cycles in WDM network", *Proc. of IEEE ICC*, pp. 2761-2765, April/May 2002.

[27] D. B. John, "Finding all the elementary circuits of a directed graph", *SIAM J. on Computing*, Vol. 4, 1975, pp 77-84.

[28] P. Batchelor etal., "Ultra high capacity optical transmission networks", *Final report of action COST 239*, 1999.

[29] D. A. Schupke, M. Jger, and R. Hlsermann, "Comparison of resilience mechanisms for dynamic services in intelligent optical networks," *Proc. of DRCN workshop*, pp. 106-113, October 2003.

[30] W.D. Grover, "The Protected Working Capacity Envelope Concept: An Alternative Paradigm for Automated Service Provisioning," /em IEEE Communications Magazine, pp. 62-69, January 2004.

[31] G. Shen and W. D. Grover, "Performance of protected working capacity envelopes based on p-cycles: Fast, simple, and scalable dynamic service provisioning of survivable services," *Proc. Asia-Pacific Optical and Wireless Communications Conference (APOC)*, November. 2004, vol. 5626.

[32] L. Ruan and F. Tang, Dynamic Establishment of Restorable Connections using p-Cycle Protection in WDM Networks, *Proc. of Broadnets*, pages 147-154, October 2005.

[33] W. D. Grover, Mesh-Based Survivable Networks. Upper Saddle River, New Jersey, USA: Prentice Hall PTR, 2003.

[34] D. S. Hochbaum, "The bounded cycle cover problem", *INFORMS Journal on Computing*, Vol. 13, pp 104-119, 2001.

[35] H. Sakauchi, Y. Okanoue, and S. Hasegawa, "Spare-channel design schemes for self-healing networks," *IEICE Trans. Comm.*, Vol. E75-B, no.7, PP. 624-633, July 1992.

[36] M. Clouqueur, and W.D.Grove, "Computational and design studies on the unavailability of mesh-restorable networks," *Proc. IEEE/VDE Design of Reliable Communication Networks 2000*, pp. 181-186, April 2000.

[37] D.A. Schupke, R.G. Prinz, "Capacity Efficiency and Restorability of Path Protection and Rerouting in WDM Networks Subject to Dual Failures," *Photonic Network Communications*, vol. 8, no. 2, pp. 191-207, September 2004.

[38] H. Choi, S. Subramaniam, and H.A. Choi, "On double-link failure recovery in wdm optical networks," *IEEE INFOCOM*, pp. 808–816, June 2002.

[39] M. Clouqueur and Wayne D. Grove, "Mesh-restorable networks with complete dual failure restorability and with selectively enhanced dual-failure restorability properties", *Proc. SPIE*, vol.4874, pp. 1-12, July 2002.

[40] M. T. Fredericks, Pallab Datta and A. K. Somani, "Evaluating Dual-failure restorability in mesh-restorable WDM optical networks", *ICCCN 2004*, pp. 309 - 314, October 2004.

[41] W. He, M. Sridharan and A. K. Somani, "Capacity optimization for tolerating double link failures in WDM mesh optical networks", *Photonic Network Communication* , vol. 9:1, pp. 99-111, 2005.

[42] A. Chandak and S. Ramasubramanian, "Dual-link failure resiliency through backup link mutual exclusion," *Proceedings of IEEE BROADNETS*, October 2005.

[43] M. Sridharan, M.V. Salapaka, and A.K. Somani, "Operating mesh-survivable wdm transport networks," *SPIE International Symposium on SPIE Terabit Optical Networking: Terabit Optical Networking*, pp. 113–123, November 2000.

[44] I.Chlamtac and A.Gumaste, "Light-Trails: A solution to IP centric communication in the optical domain," *Second Intl. Workshop on Quality of Service in Multiservice IP Networks (QoS-IP 2003)*,Springer-Verlag Heidelberg, pp.634-644.

[45] P. Gambini *et al.*, "Transparent optical packet switching: network architecture and demonstrators in the KEOPS project," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, pp. 1245–1259, Sept 1998.

[46] Y. Yamada *et al.*, "Optical ouput buffered ATM switch prototype based on FRONTIER-NET architecture," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, pp. 1298–1307, Septemer 1998.

[47] M. Mahony, D. Simeonidou, D. Hunter, and A. Tzanakaki, "The application of optical packet switching in future communication networks," *IEEE Communication Magazine*, pp. 128–135, March 2001.

[48] M. Yoo and C. Qiao, "Optical burst switching (OBS) - a new paradigm for an optical internet," *J. High Speed Networks (JHSN)*, vol. 8, no. 1, pp. 69–84, 1999.

[49] J. Turner, "Terabit burst switching," *J. High Speed Networks (JHSN)*, vol. 8, no. 1, 1999.

[50] A. Ge, F. Callegati, and L. Tamil, "On optical burst switching and self-similar traffic," *IEEE Communication Letters*, vol. 4, no. 3, pp. 98–100, March 2000.

[51] S. Verma, H. Chaskar, and R. Ravikanth, "Optical burst switching: A viable solution for terabit ip backbone," *IEEE Network*, pp. 48–53, November/December 2000.

[52] J. Fang, W. He and A. k. Somani, "Optimal light trail design in WDM optical networks", *IEEE ICC 2004*, Vol. 3, pp. 1699-1703, June 2004.